UBND TỈNH ĐIỆN BIÊN
TIỂU BAN AN TOÀN AN NINH MẠNG

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

Số: 2265 /CV-TBATANM
V/v phòng ngừa tấn công mạng bằng virus mã hóa dữ liệu và đòi tiền chuộc

Điện Biên, ngày 3 tháng 8 năm 2022

Kính gửi:
- Các sở, ban, ngành, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các công ty, doanh nghiệp trên địa bàn tỉnh.

Qua trao đổi với các cơ quan chuyên trách về an ninh mạng và nắm tình hình liên quan đến công tác bảo đảm an ninh, an toàn thông tin, Công an tỉnh Điện Biên thông báo đến các sở, ban, ngành, đoàn thể, UBND các huyện, thị xã, thành phố, các doanh nghiệp *(sau đây gọi tắt là các cơ quan, đơn vị)* trên địa bàn tỉnh về đợt tấn công của nhóm tin tặc sử dụng các loại virus mã hóa dữ liệu, đòi số tiền chuộc. Cụ thể như sau:

Hình thức tấn công **Ransomeware** (VIRUS đòi tiền chuộc): là cách gọi tên của dạng mã độc mới nhất và có tính nguy hiểm cao bởi nó sẽ mã hóa toàn bộ các file word, excel và các tập tin khác trên máy tính bị nhiễm làm cho người dùng không thể mở được file do bị mã hóa và yêu cầu người nhiễm mã độc trả một số tiền chuộc nhất định. Các loại mã độc rất nguy hiểm, khi bị nhiễm thì rất khó khôi phục dữ liệu. Một số trường hợp có thể thực hiện được nhưng tốn nhiều thời gian, chi phí và không thể khôi phục lại được toàn bộ dữ liệu.

Phiên bản mã độc mới đã phát hiện tại một số cơ quan, đơn vị trên địa bàn tỉnh trong đợt tấn công mạng giữa năm 2022 chủ yếu là các virus mã hóa dữ liệu dạng đuôi *".hhwq"* và *".kruu"*. Các virus này thường tấn công chủ yếu vào các file ảnh, văn bản, hệ thống như: *.doc, .docx, .excel, .exe, .png, .jpeg, .psd, .pdf, .xls, .xlsx*... Các đối tượng hacker thường đòi số tiền chuộc từ 400$ đến 5000$ trên một máy tính chứa dữ liệu bị mã hóa.

Các phương thức lây lan chủ yếu của các virus mã hóa trên: [1]Gửi tệp tin nhiễm mã độc kèm theo thư điện tử, khi người sử dụng kích hoạt tệp tin đính kèm thư điện tử sẽ làm lây nhiễm mã độc vào máy tính; [2]Gửi thư điện tử hoặc tin nhắn điện tử có chứa đường dẫn đến phần mềm bị giả mạo bởi mã độc Ransomware và đánh lừa người sử dụng truy cập vào đường dẫn này để vô ý tự cài đặt mã độc lên máy tính; [3]Gửi kèm trong file crack *(bẻ khóa)* của phần mềm không có bản quyền, các phần mềm không có uy tín; [4]Lây lan qua các thiết bị lưu trữ, sao chép dữ liệu, chuyển giao dữ liệu...

Để bảo đảm an toàn, an ninh mạng, chủ động phòng ngừa, ngăn chặn hoạt động tấn công mạng của các nhóm tin tặc, hacker. Công an tỉnh đề nghị:

1. Tăng cường các biện pháp phòng ngừa, hạn chế tối đa khả năng bị nhiễm mã độc.

- Thường xuyên cập nhật bản vá, phiên bản mới nhất cho hệ điều hành và

phần mềm chống mã độc *(Kaspersky, Symmatec, Avast, AVG, MSE, Bkav, CMC, ...)*. Khuyến khích sử dụng các phiên bản phần mềm phòng chống mã độc có chức năng đảm bảo an toàn khi truy cập mạng Internet và phát hiện mã độc trực tuyến.

- Cần chú ý cảnh giác với các tệp tin đính kèm, các đường dẫn *(link)* được gửi đến qua thư điện tử hoặc tin nhắn, hạn chế tối đa việc truy cập vào các đường dẫn này vì tin tặc có thể đánh cắp hoặc giả mạo hòm thư điện tử người gửi phát tán các kết nối chứa mã độc.

- Sử dụng phần mềm diệt virus hoặc website check virus để kiểm tra các tệp tin được gửi qua thư điện tử, tải từ trên mạng về trước khi kích hoạt. Nếu không cần thiết hoặc không rõ nguồn gốc thì không kích hoạt các tệp tin này. *(Ví dụ: khi tải file **A.rar** về máy, có thể upload tệp tin này lên website https://www.virustotal.com để check virus trước khi sử dụng).*

- Tắt chế độ tự động mở, chạy các tệp tin đính kèm theo thư điện tử.

2. Tiến hành sao lưu dữ liệu định kỳ, thường xuyên để có thể khôi phục dữ liệu khi máy tính bị Ransomware gây hại, các cơ quan, đơn vị tham khảo một số biện pháp sau:

- Sử dụng đĩa CD ROM, DVD ROM để sao lưu dữ liệu là phương pháp đơn giản và an toàn, tuy nhiên không được thuận tiện khi sử dụng lâu dài và thường xuyên.

- Sử dụng các ổ lưu trữ USB, ổ đĩa cắm ngoài, ổ chia sẻ mạng v.v... Cần chú ý dữ liệu trong các ổ lưu trữ này hoàn toàn có thể bị ảnh hưởng nếu kết nối vào máy tính đã bị nhiễm mã độc Ransomware. Do vậy phải đảm bảo máy chưa bị nhiễm mã độc trước khi sao lưu hoặc khởi động máy tính từ ổ đĩa khởi động ngoài khi thực hiện sao lưu để đảm bảo an toàn.

- Sử dụng các công cụ, giải pháp chuyên dụng để sao lưu như: các máy chủ quản lý tệp tin, máy chủ sao lưu từ xa, các công cụ lưu trữ đám mây cho phép khôi phục lịch sử thay đổi của tập tin mà khi xảy ra sự cố có thể khôi phục lại từ thời điểm trước đó.

3. Xử lý khi phát hiện bị lây nhiễm mã độc: Khi mã độc Ransomware lây nhiễm vào máy tính sẽ tiến hành mã hóa các tệp tin dữ liệu, khóa máy tính của người dùng khiến người dùng không can thiệp để tắt tiến trình đang chạy. Quá trình mã hóa cần thời gian dài vì vậy việc phản ứng nhanh chóng khi phát hiện ra sự cố sẽ giúp giảm thiểu thiệt hại cho các dữ liệu trên máy bị nhiễm và có thể khôi phục các dữ liệu bị mã hóa. Do đó, khi phát hiện ra dấu hiệu bị lây nhiễm mã độc Ransomware cần phải nhanh chóng thực hiện các thao tác sau:

- Nhanh chóng tắt máy tính *(Tắt nguồn điện, không sử dụng chức năng shutdown của hệ điều hành).*

- Phải sử dụng khởi động từ hệ thống sạch khi thực hiện sao lưu các dữ liệu chưa bị mã hóa *(Chế độ Safe mode, win PE...).*

- Trong trường hợp không cần cứu dữ liệu, cần format ổ cứng và cài đặt lại toàn bộ hệ thống, cài phần mềm diệt virus phiên bản mới nhất và tiến hành quét toàn bộ dữ liệu trên máy tính trước khi sao chép lại các dữ liệu vào máy tính.

Đề nghị các cơ quan, đơn vị tăng cường theo dõi, thực hiện các nội dung trên; Khi phát hiện xảy ra sự cố về mã độc Ransomware cần liên hệ với Công an tỉnh *(Qua phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao Công an tỉnh, số điện thoại: 0692.489.489)* để được hướng dẫn, phối hợp xử lý./.

Nơi nhận:
- Như trên;
- Trưởng tiểu ban ATANM;
- Lưu: VT, CAT (PA05).

KT. TRƯỞNG TIỂU BAN
PHÓ TRƯỞNG TIỂU BAN

Giám đốc Công an tỉnh
Đại tá Ngô Thanh Bình