**Cách phòng ngừa và biện pháp xử lý khi phát hiện máy tính bị lây nhiễm mã độc Ransomware**

Trong thời gian gần đây máy tính trong nhiều cơ quan tổ chức tại Việt Nam đã xảy ra lây nhiễm các phiên bản mới của mã độc Ransomware như CTB Locker/Critroni hoặc Onion. Đây là loại mã độc rất nguy hiểm, có thể dẫn đến mất mát dữ liệu lớn trong các cơ quan, tổ chức và cá nhân, đặc biệt khi bị nhiễm mã độc và các tài liệu đã bị mã hóa thì không thể khôi phục dữ liệu. Hiện nay, tại Gia Lai đã có một số hệ thống mạng nội bộ (LAN) của đơn vị, địa phương bị lây nhiễm mã độc Ransomware, hậu quả là bị chiếm quyền kiểm soát, bị thu thập thông tin hoặc thậm chí bị mã hóa toàn bộ máy tính. Để đảm bảo an toàn thông tin trên hệ thống do các đơn vị, địa phương đang quản lý, Trung tâm Công nghệ thông tin và Truyền thông tỉnh Gia Lai đưa ra các giải pháp phòng ngừa và biện pháp xử lý khi phát hiện máy tính bị lây nhiễm mã độc Ransomware

**1. Ransomware là gì?**

Đây là cách gọi tên của dạng mã độc mới nhất và có tính nguy hiểm cao độ đối với nhân viên văn phòng, bởi khi bị lây nhiễm nó sẽ mã hóa toàn bộ các tập tin tài liệu: MS Word (.doc, .docx), MS Excel (.xls, .xlsx), dạng PDF (.pdf), file ảnh (.gif, .jpg, .png,…), file nén (.zip) và các tập tin khác trên máy tính bị nhiễm làm cho nạn nhân không thể mở được file.

Một trong những đại diện nổi tiếng của mã độc Ransomware này là CTBLocker/Critroni hoặc Onion. Các chuyên gia của Kaspersky Lab nhận dạng các trường hợp bị nhiễm nhiều nhất tại Việt Nam là do Trojan-Ransom.Win32.Onion gây nên.

**2. Các phương pháp lây nhiễm:**

Một số phương pháp lây lan chủ yếu của mã độc Ransomware là:

- 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.
- 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.
- Ngoài ra máy tính còn có thể bị nhiễm thông qua các con đường khác như lây lan qua các thiết bị lưu trữ; lây qua cài đặt phần mềm; sao chép dữ liệu, phần mềm; truy cập từ các trang web không rõ nguồn gốc; các phần mềm game trò chơi có chứa mã độc,...

**3. Hình thức hoạt động của mã độc Ransomware:**

Thông thường, sau khi xâm nhập vào máy tính, nó sẽ tiến hành mã hóa dữ liệu bằng cách sử dụng thuật toán mã hóa với khóa công khai (public-key).

Nhiều mã độc Ransomware được ngụy trang khá tốt, đôi khi chúng sẽ

đưa ra những cảnh báo giả cho người dùng để mua bản quyền phần mềm,…; một số trường hợp khác, mã độc Ransomware sẽ thâm nhập sâu vào bên trong hệ thống của máy rồi hiển thị một thông báo; một số loại mã độc còn tiến hành khóa máy tính nạn nhân không cho sử dụng hoặc đưa ra các cảnh báo. Sau đó mã độc sẽ yêu cầu người bị hại thanh toán qua mạng (thẻ tín dụng hoặc bitcoin) để lấy mật khẩu giải mã các tệp đã bị mã hóa trái phép.

**4. Một số biện pháp phòng ngừa để hạn chế khả năng nhiễm mã độc Ramsomware:**

- Thiết lập quyền người sử dụng không ở chế độ quản trị hệ thống (Administrator) và thiết lập các cấu hình nhằm bảo vệ file với quyền không cho phép xóa, sửa các file quan trọng một cách tự động. Ngăn chặn việc thực thi các ứng dụng từ các thư mục chứa dữ liệu quan trọng. Thường xuyên cập nhật bản vá, phiên bản mới nhất cho hệ điều hành và phần mềm chống mã độc (Kaspersky, Synmatec, Avast, AVG, MSE, Bkav, CMC, v.v...). Nên sử dụng các phiên bản phần mềm phòng chống mã độc có chức năng đảm bảo an toàn khi truy cập Internet và phát hiện mã độc trực tuyến.

- Thường xuyên sử dụng phần mềm diệt mã độc, virus kiểm tra máy tính, ổ lưu trữ để phát hiện sớm nếu xuất hiện mã độc trên thiết bị.

- 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 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.

- Đảm bảo các tính năng bảo vệ thời gian thực như: System Watcher (giám sát hệ thống) của chương trình Kaspersky, Real time Protection của Bkav Pro,…

- Tắt chế độ tự động mở, chạy các tệp tin đính kèm theo thư điện tử. Cấu hình hạn chế truy cập đến các thư mục chia sẻ trong mạng.

- Bật tính năng System Protection (System Restore) cho tất cả các ổ đĩa.

- Bật tính năng của thiết bị tường lửa (Firewall) hiện có của đơn vị chặn các địa chỉ IP lạ từ các nước khác truy nhập vào hệ thống.

**5. Thực hiện sao lưu định kỳ dữ liệu:**

- Cần tiến hành sao lưu và bảo vệ định kỳ dữ liệu thường xuyên bằng các thiết bị rời để có thể khôi phục dữ liệu khi máy tính bị Ransomware gây hại, các cơ quan, đơn vị có thể tham khảo một số biện pháp sau:

- Sử dụng đĩa CD, DVD 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...

**6. Xử lý khi phát hiện bị lây nhiễm mã độc:**

Khi mã độc Ransomware lây nhiễm vào máy tính bị hại, mã độc sẽ tiến hành mã hóa các tệp tin dữ liệu, khóa máy tính của người dùng để người dùng không can thiệp để tắt tiến trình đang chạy. Do qua trình mã hóa cần sẽ được thực hiện trong thời gian dài chính vì vậy việc phản ứng nhanh chóng khi phát hiện ra sự cố sẽ giúp giảm thiểu thiệt hại cho các dữ liệu chứa trên máy bị nhiễm và giúp các chuyên gia có thể khôi phục các dữ liệu bị mã hóa. Do đó, đối với các máy tính cá nhân 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 hệ thống sạch từ USB, DVD, CD,...để khởi động máy tính bị nhiễm trước khi thực hiện sao lưu các dữ liệu chưa bị mã hóa.

- Cài đặt lại toàn bộ hệ thống, cài phần mềm diệt virus cập nhật 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.

**7. Khôi phục các file bị ảnh hưởng:**

Hiện nay vẫn chưa có một phần mềm hữu hiệu hoặc dịch vụ thương mại nào cho phép giải mã các file đã bị mã hóa. Mặc dù không có khả năng giải mã các file đã bị mã độc mã hóa, Tuy nhiên, trong một số trường hợp có thể sử dụng các phần mềm khôi phục dữ liệu như: FTK, EaseUs, R-STUDIO, RectorDecryptor, XoristDecryptor, RakhniDecryptor tại địa chỉ http://support.kaspersky.com/viruses/utility để khôi phục các file nguyên bản đã bị xóa hay mã hóa hoặc tải phần mềm Anti Ransomware của Bkav tại địa chỉ http://www.bkav.com.vn/download/BkavRS.exe và phần mềm ShadowExplore tại địa chỉ http://www.shadowexplorer.com/uploads/ShadowExplorer-0.9-portable.zip để khôi phục dữ liệu cũ mà Windows đã tạo bản sao trước đó.

Trường hợp, Quý cơ quan, đơn vị không đảm bảo năng lực để xử lý sự cố này thì phải yêu cầu sự hỗ trợ của các chuyên gia về an toàn thông tin nhằm giảm thiểu các thiệt hại khi xảy ra sự cố. Các đơn vị có thể gửi các tập tin đáng ngờ theo dạng nén và mật khẩu qua địa chỉ sau:

- Kaspersky: newvirus@kaspersky.com
- Bkav Pro: BkavPro@bkav.com

Hoặc liên hệ Trung tâm Công nghệ thông tin và Truyền thông tỉnh Gia Lai để hỗ trợ kỹ thuật.