Cảnh báo Ransomware WanaCrypt0r đang tấn công trên diện rộng

Hiện tại, mã độc ransomware có tên WannaCry (WanaCrypt0r) đang khai thác lỗ hổng trên HĐH Windows để tấn công vào các máy tính với mục tiêu mã hóa dữ liệu để đòi tiền chuộc, ảnh hưởng tới nhiều tổ chức, cá nhân trên phạm vi toàn cầu. Công ty CP NamTrường sơn HN có thông báo hướng dẫn các cá nhân, tổ chức thực hiện các biện pháp phòng tránh và xử lý khẩn cấp mã độc này như sau:

I. Đối với cá nhân:

- Liên hệ với quản trị mạng hoặc thực hiện cập nhật ngay các phiên bản hệ điều hành windows đang sử dụng.
- Cập nhật ngay các chương trình Antivius đang sử dụng. Đối với các máy tính không có phần mềm Antivirus cần tiến hành cài đặt ngay phần mềm Antivirus có bản quyền.
- Cẩn trọng khi nhận được email có đính kèm và các đường link lạ được gửi trong email, trên các mạng xã hội, công cụ chat…

- Chú ý thận trọng khi mở các file đính kèm ngay cả khi nhận được từ những địa chỉ quen thuộc. Sử dụng các công cụ kiểm tra phần mềm độc hại trực tuyến hoặc có bản quyền trên máy tính với các file này trước khi mở ra.
- Không mở các đường dẫn có đuôi .hta hoặc đường dẫn có cấu trúc không rõ ràng, các đường dẫn rút gọn link, nếu có nghi ngờ cần liên hệ với cán bộ phụ trách IT ngay.
- Thực hiện biện pháp lưu trữ (backup) dữ liệu quan trọng ngay lập tức.

II. Đối với các quản trị viên hệ thống

- Thực hiện lệnh quét virusscan cho vùng Critical Areas, nếu phát hiện malware dạng ***MEM:Trojan.Win64.EquationDrug.gen*** cần khởi động lại máy tính ngay.
- Thực hiện biện pháp lưu trữ (backup) dữ liệu quan trọng ngay.
- Cập nhật đầy đủ cho các máy chủ/máy trạm đang sử dụng hệ điều hành Windows, đặc biệt là bản vá lỗi EternalBlue (MS17-010) theo đường dẫn dưới đây :
  Security Update for Microsoft Windows SMB Server (MS17-010 – Critical)
- Riêng đối với các máy tính sử dụng Windows XP, sử dụng bản vá dưới đây :
  Security Update for Windows XP SP3 (KB4012598)
  hoặc tìm kiếm theo từ khóa bản cập nhật ***KB4012598*** trên trang chủ của Microsoft.
- Tạo các bản snapshot đối với các máy chủ ảo hóa đề phòng việc bị tấn công.
- Kiểm tra tình trạng hoạt động của phần mềm diệt virus đang được cài đặt với đầy đủ các tính năng bảo vệ, đặc biệt là tính năng **System Watcher** , thông báo người dùng không được tự ý tắt hay gỡ bỏ.
- Cập nhật cơ sở dữ liệu mới nhất cho các máy chủ, máy trạm đã được trang bị hệ thống Antivirus Endpoint Security.
- Kiểm tra ngay các máy chủ và tạm thời khóa (block) các dịch vụ đang sử dụng các cổng 445/137/138/139.
- Tận dụng các công cụ, giải pháp an toàn thông tin để theo dõi, giám sát và bảo vệ hệ thống trong thời điểm nhạy cảm này.
- Ngăn chặn (block) việc sử dụng các phần mềm chia sẻ file ngang hàng Tor trong hệ thống mạng.

- Cảnh báo tới người dùng trong đơn vị và thực hiện các biện pháp như nêu trên đối với người dùng.
- Trong trường hợp phát hiện máy tính bị lây nhiễm, không làm theo các hướng dẫn của hacker để tránh mất tiền và lây nhiễm virus thêm.
- Xác định và ngắt máy tính bị lây nhiễm khỏi hệ thống mạng, update chương trình diệt virus và quét lại toàn bộ máy tính để làm sạch virus trước khi cài đặt lại.
- Liên hệ ngay với các cơ quan chức năng cũng như các tổ chức, doanh nghiệp trong lĩnh vực an toàn thông tin để được hỗ trợ khi cần thiết.

- **Một số thông tin tham khảo :**
  - Mã độc WannaCry ban đầu chỉ hoạt động khi người dùng click vào một đường link giả mạo hay một tập tin giả, tuy nhiên biến thể WanaCrypt0r hiện tại đã lợi dụng các lỗ hổng Windows để lây lan rộng rãi. Thông qua việc khai thác lỗ hổng EternalBlue của dịch vụ SMB, mã độc cài đặt một phần mềm backdoor NSA mang tên DoublePulsat, từ đó WannaCry được lây nhiễm vào máy rồi tự động lây lan nhanh chóng đến các máy tính trong cùng một mạng.
  - Thông báo của cục An toàn thông tin – Bộ TT&TT về mã độc này : http://ais.gov.vn/tin-noi-bat/cuc-an-toan-thong-tin-canh-bao-va-khuyen-nghi-xu-ly-gap-toi-nguoi-dan-doanh-nghiep-va-cac-to-chuc.htm
  - Tham khảo thông báo mô tả và cảnh báo của hãng bảo mật Kaspersky Lab : https://blog.kaspersky.com/wannacry-ransomware/16518/

Do tính chất nguy hiểm của mã độc, để đề phòng việc lây nhiễm và xảy ra sự cố mất dữ liệu nghiêm trọng, rất mong Quý Khách hàng chú ý các biện pháp phòng chống và cảnh báo nêu trên.