

Bộ TT&TT hướng dẫn xử lý khẩn cấp mã độc WannaCry

11:36 15/05/2017

Bộ TT&TT vừa phát đi cảnh báo mã độc có tên WannaCry khai thác một số lỗ hổng trên hệ điều hành Windows để tấn công vào các máy tính với mục tiêu mã hóa dữ liệu để đòi tiền chuộc.



Khẩn cấp phòng ngừa, ngăn chặn sự tấn công của mã độc WannaCry (Ảnh: VTV)

Theo Cổng TTĐT Bộ TT&TT, hiện tại, mã độc có tên là WannaCry khai thác một số lỗ hổng trên hệ điều hành 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.

Cục An toàn thông tin – Bộ Thông tin và Truyền thông hướng dẫn các tổ chức, cá nhân thực hiện biện pháp xử lý khẩn cấp mã độc này.

Đối với cá nhân:

Thực hiện cập nhật ngay các phiên bản hệ điều hành windows đang sử dụng. Riêng đối với các máy tính sử dụng Windows XP, sử dụng bản cập nhật mới nhất dành riêng cho sự vụ này tại: https://www.microsoft.com/en-us/download/details.aspx?id=55245&WT.mc_id=rss_windows_allproducts hoặc tìm kiếm theo từ khóa bản cập nhật KB4012598 trên trang chủ của Microsoft.

Cập nhật ngay các chương trình Antivirus đang sử dụng. Đối với các máy tính không có phần mềm Antivirus cần tiến hành cài đặt và sử dụng ngay một 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...

Cẩn 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.

Thực hiện biện pháp lưu trữ (backup) dữ liệu quan trọng ngay.

Đối với tổ chức, doanh nghiệp (cụ thể với các quản trị viên hệ thống):

Kiểm tra ngay lập tức các máy chủ và tạm thời khóa (block) các dịch vụ đang sử dụng các cổng 445/137/138/139.

Tiến hành các biện pháp cập nhật sớm, phù hợp theo từng đặc thù cho các máy chủ windows của tổ chức. Tạo các bản snapshot đối với các máy chủ ảo hóa để phòng việc bị tấn công.

Có biện pháp cập nhật các máy trạm đang sử dụng hệ điều hành Windows.

Cập nhật cơ sở dữ liệu cho các máy chủ Antivirus Endpoint đang sử dụng. Đối với hệ thống chưa sử dụng các công cụ này thì cần triển khai sử dụng các phần mềm Endpoint có bản quyền và cập nhật mới nhất ngay cho các máy trạm.

Tận dụng các giải pháp đảm bảo an toàn thông tin đang có sẵn trong tổ chức như Firewall, IDS/IPS, SIEM... để theo dõi, giám sát và bảo vệ hệ thống trong thời điểm nhạy cảm này. Cập nhật các bản cập nhật từ các hãng bảo mật đối

với các giải pháp đang có sẵn. Thực hiện ngăn chặn, theo dõi domains đang được mã độc WannaCry sử dụng, để xác định được các máy tính bị nhiễm trong mạng để có biện pháp xử lý kịp thời:

o <http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/>

Cân nhắc việc ngăn chặn (block) việc sử dụng Tor trong mạng nếu doanh nghiệp, tổ chức.

Thực hiện biện pháp lưu trữ (backup) dữ liệu quan trọng ngay.

Cảnh báo tới người dùng trong tổ chức và thực hiện các biện pháp như nêu trên đối với người dùng.

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.

PV