UBND TỈNH NINH THUẬN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 761 /STTTT-CNTT
V/v cảnh báo và khuyến nghị xử lý gấp về mã độc Wanna Cry của nhóm tin tặc Shadow Brokers

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

Ninh Thuận, ngày 16 tháng 5 năm 2017

Kính gửi:
- Các cơ quan thuộc Tỉnh ủy;
- Các Sở, ban ngành thuộc Ủy ban nhân dân tỉnh;
- Ủy ban nhân dân các huyện, thành phố;
- Ủy ban nhân dân các xã, phường, thị trấn;
- Các doanh nghiệp viễn thông trên địa bàn tỉnh.

Tiếp nhận Công văn số 123/VNCERT-ĐPƯC ngày 24/4/2017 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam về các phương thức tấn công khai thác hệ thống mới của nhóm tin tặc Shadow Brokers;

Ngày 09/5/2017, Sở Thông tin và Truyền thông đã ban hành Công văn số 724/STTTT-CNTT về việc cảnh báo về phương thức tấn công khai thác hệ thống mới của nhóm tin tặc Shadow Brokers.

Hiện tại, mã độc 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.

Nhằm triển khai kịp thời theo hướng dẫn của Cục An toàn thông tin, Sở Thông tin và Truyền thông đề nghị các tổ chức, cá nhân thực hiện biện pháp xử lý khẩn cấp mã độc này như sau:

1. 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 Antivius 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...

- Cần 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.

2. Đối với tổ chức, doanh nghiệp (cụ thể với các quản trị mạng):

- 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 bị mã độc WannaCry sử dụng, để là xác định được các máy tính bị nhiễm trong mạng để có biện pháp xử lý kịp thời.

- Cân nhắc việc ngăn chặn (block) việc sử dung 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.

3. Đầu mối điều phối ứng cứu

Ngay khi phát hiện sự cố với các phương thức tấn công mới, Quý đơn vị thông báo ngay về:

- Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam

Địa chỉ: tầng 5, Tòa nhà 115 Trần Duy Hưng, Cầu Giấy, Hà Nội

Điện thoại: 04 3640 4423 (số máy lẻ 112), 0934 424 009

Thư điện tử: ir@vncert.gov.vn

- Sở Thông tin và Truyền thông tỉnh Ninh Thuận

Địa chỉ: 17 Nguyễn Trãi, phường Kinh Dinh, thành phố Phan Rang-Tháp Chàm, tỉnh Ninh Thuận.

Điện thoại: 068 3922753

Thư điện tử: sotttt@ninhthuan.gov.vn

Trân trọng./.

Nơi nhận:
- Như trên;
- Trung tâm CNTT-TT;
- Lưu: VT, CNTT.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH NINH THUẬN

Đào Xuân Kỳ