UBND TỈNH KHÁNH HÒA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1319/STTTT-CNTT

Khánh Hòa, ngày 24 tháng 7 năm 2018

V/v cảnh báo, ngăn chặn kết nối và xóa các tập tin mã độc tấn công có chủ đích

Kính gửi:
- Các Sở, ban, ngành;
- Ủy ban nhân dân các huyện, thị xã, thành phố;
- Các đơn vị sự nghiệp trực thuộc Ủy ban nhân dân tỉnh;
- Các cơ quan ngành dọc Trung ương.

Sở Thông tin và Truyền thông nhận được Công văn số 234/VNCERT-ĐPƯC ngày 21/7/2018 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) – Bộ Thông tin và Truyền thông về việc theo dõi, ngăn chặn kết nối và xóa các tập tin mã độc tấn công có chủ đích vào ngân hàng và các tổ chức hạ tầng quan trọng quốc gia.

Theo nội dung cảnh báo của Trung tâm VNCERT tại Công văn nêu trên, Trung tâm VNCERT đã ghi nhận các hình thức tấn công có chủ đích của các tin tặc nhằm vào hệ thống thông tin của một số ngân hàng và hạ tầng quan trọng quốc gia tại Việt Nam. Mục đích chính của tin tặc là đánh cắp các thông tin quan trọng của ngân hàng và các tổ chức hạ tầng quan trọng quốc gia. Với việc tin tặc sử dụng các kỹ thuật cao để tấn công, các hệ thống bảo vệ an toàn thông tin của các ngân hàng hoặc tổ chức hạ tầng quan trọng sẽ khó phát hiện kịp thời và đồng thời giúp tin tặc duy trì quyền kiểm soát hệ thống thông tin.

Để ngăn chặn các rủi ro có thể xảy ra, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, địa phương khẩn trương thực hiện các nội dung sau:

1. Theo dõi và ngăn chặn kết nối đến các máy chủ C&C có địa chỉ IP sau:

a) 38.132.124.250

b) 89.249.65.220

2. Rà quét hệ thống máy chủ tại các cơ quan, thực hiện xóa các thư mục và tập tin mã độc có kích thước tương ứng:

a) syschk.ps1 (318 KB (326,224 bytes))

- MD5: 26466867557F84DD4784845280DA1F27

- SHA-1:ED7FCB9023D63CD9367A3A455EC94337BB48628A

b) hs.exe (259 KB (265,216 byte))

- MD5: BDA82F0D9E2CB7996D2EEFDD1E5B41C4

- SHA-1: 9FF715209D99D2E74E64F9DB894C114A8D13229A

Hướng dẫn kiểm tra mã MD5, SHA-1 của tập tin và cách thức xóa tập tin chứa mã độc *chi tiết tại Phụ lục đính kèm Công văn này*.

3. Khẩn trương thông báo nội dung văn bản này đến tất cả các cơ quan, đơn vị trực thuộc để tổ chức triển khai thực hiện.

Sau khi triển khai các biện pháp nêu trên, đề nghị Quý cơ quan báo cáo kết quả thực hiện và tổng hợp tình hình thông tin mã độc phát hiện, xử lý được (nếu có) về Sở Thông tin và Truyền thông qua phần mềm E-Office hoặc địa chỉ thư điện tử cntt.stttt@khanhhoa.gov.vn **trước 15 giờ ngày 27/7/2018** để tổng hợp, báo cáo Ủy ban nhân dân tỉnh và Trung tâm VNCERT.

Quá trình thực hiện nếu có vướng mắc hoặc cần hỗ trợ, đề nghị Quý cơ quan liên hệ đầu mối Thường trực Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa để phối hợp xử lý:

- Phòng Công nghệ thông tin – Sở Thông tin và Truyền thông;

- Địa chỉ: Nhà A1 Khu liên cơ số 01 Trần Phú, thành phố Nha Trang;

- Điện thoại: 0258.3563533;

- Thư điện tử: cntt.stttt@khanhhoa.gov.vn

Sở Thông tin và Truyền thông đề nghị Quý cơ quan quan tâm thực hiện.

Trân trọng./.

Nơi nhận:
- Như trên (VBĐT);
- UBND tỉnh (VBĐT, để b/c);
- Trung tâm VNCERT (VBĐT, để b/c);
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Ký bởi: Nguyễn Thị Trung Thu
Email: nttthu@khanhhoa.gov.vn
Cơ quan: Sở Thông tin và Truyền thông, Tỉnh Khánh Hòa
Thời gian ký: 24.07.2018

Nguyễn Thị Trung Thu

Phụ lục
Hướng dẫn kiểm tra mã MD5, SHA-1 của tập tin
và cách thức xoá tập tin chứa mã độc
(Kèm theo Công văn số 1319/STTTT-CNTT ngày 24/7/2018
của Sở Thông tin và Truyền thông)

1. Hướng dẫn kiểm tra mã hash MD5, SHA-1:

a) Download phần mềm tại: http://www.nirsoft.net/utils/hashmyfiles.zip (các đơn vị có thể sử dụng các công cụ kiểm tra mã hash tin tưởng khác).

b) Kiểm tra: Giải nén tập tin hashmyfiles.zip trên, tiến hành mở file "HashMyFiles.exe". Nhấn vào File -> Add Files; trỏ đến file cần kiểm tra mã Hash. Mã MD5 và SHA-1 sẽ hiển thị bên khung chương trình. Thực hiện đối chiếu mã MD5 và SHA-1 tương ứng trong Công văn đi kèm và thực hiện *Mục 2 - Hướng dẫn gỡ bỏ tệp tin chứa mã độc*.

2. Hướng dẫn gỡ bỏ tập tin chứa mã độc:

a) Xác định mã độc: Nếu mã MD5 và SHA-1 trùng nhau thì tập tin trên máy tính là phần mềm có chứa mã độc. Nếu không trùng thì chưa khẳng định 100% nó không phải là mã độc. Có thể không xoá trong trường hợp này nhưng cần trích xuất tệp tin và thực hiện phân tích chuyên sâu. Đối với các máy có chứa file mã độc cần ngay lập tức cô lập và báo cáo cho Cơ quan điều phối quốc gia (Trung tâm VNCERT)

b) Cách xoá tập tin chứa mã độc: Do tập tin này đang được thực thi nên trên máy nên cần dừng hoặc tắt tiến trình này trước khi xoá. Trước tiên, cần tải phần mềm miễn phí có tên "Process Explorer" của Microsoft tại địa chỉ bên dưới: https://download.sysinternals.com/files/ProcessExplorer.zip

Sau khi tải về, giải nén, chạy file "procexp.exe" và thực hiện các bước sau:

- Tiến hành tìm kiếm các tiến trình tương ứng trong Công văn ở trên và nhấn chuột phải chọn Properties, tại mục Explore để mở Path của tệp tin, thư mục

Autostart Location để hiển thị vị trí các giá trị Registry mà mã độc đã tạo hoặc thay đổi giá trị.

- Trích xuất các tệp tin nghi ngờ hoặc mã độc này bằng cách nhấn vào Create Dump, copy nén và đặt pass khó cho file thực thi để phục vụ công tác điều tra.

- Tiến hành tìm kiếm các tiến trình tương ứng trong Công văn ở trên và nhấn chuột phải chọn "Suspend" hoặc "Kill Process". Sau khi chọn xong, vào đường dẫn tương ứng để xoá. Kiểm tra các giá trị Registry đã được tạo hoặc thay đổi và xóa./.