UBND TỈNH ĐỒNG NAI
SỞ Y TẾ

Số: 3234 /SYT-VP
V/v triển khai thực hiện Công văn số 420/CNTT-CSHT ngày 24/7/2018 của Cục CNTT Bộ Y tế.

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

Đồng Nai, ngày 30 tháng 7 năm 2018

VĂN BẢN ĐIỆN TỬ
KHÔNG GỞI VĂN BẢN GIẤY

Kính gửi: Giám đốc, Thủ trưởng các đơn vị trực thuộc.

Thực hiện Công văn số 420/CNTT-CSHT ngày 24/7/2018 của Cục Công nghệ thông tin Bộ Y tế về việc theo dõi, ngăn chặn kết nối và xóa các tập tin mã độc tấn công có chủ đích (*đính kèm Công văn*).

Giám đốc Sở Y tế yêu cầu Giám đốc, Thủ trưởng các đơn vị trực thuộc chỉ đạo các tổ chức, cá nhân của đơn vị mình phụ trách về công nghệ thông tin được biết và thực hiện theo đúng các nội dung chỉ đạo của công văn.

Yêu cầu Giám đốc, Thủ trưởng các đơn vị trực thuộc triển khai thực hiện theo sự chỉ đạo, trong quá trình thực hiện có khó khăn vướng mắc liên hệ với Cục Công nghệ thông tin - Bộ Y tế để được hỗ trợ./.

Nơi nhận:
- Như trên;
- Website SYT;
- Lưu: VT,VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH ĐỒNG NAI

Phan Huy Anh Vũ

Số 2 - Phan Đình Phùng, phường Quang Vinh, thành phố Biên Hoà, tỉnh Đồng Nai
ĐT: (02513) 942641, Fax: (02513) 847269, Email: syt@dongnai.gov.vn, Website: syt.dongnai.gov.vn

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

Số: 420/CNTT-THDL
V/v theo dõi, ngăn chặn kết nối và xoá các tập tin mã độc tấn công có chủ đích.

Hà Nội, ngày 24 tháng 7 năm 2018

Kính gửi:
- Tổng Cục Dân số và các Vụ, Cục, Văn phòng Bộ, Thanh tra Bộ;
- Các đơn vị trực thuộc Bộ Y tế;
- Sở Y tế các tỉnh, thành phố trực thuộc Trung ương.

(Sau đây gọi tắt là các đơn vị)

Căn cứ Công văn số 234/VNCERT-KTHT&GS của Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam ngày 21/7/2018 về việc theo dõi, ngăn chặn kết nối và xoá các tập tin mã độc tấn công có chủ đích vào ngân hàng và các tổ chức hạ tầng quan trọng quốc gia.

Căn cứ Quyết định số 632/QĐ-TTg ngày 10/5/2017 của Thủ tướng Chính phủ về Ban hành danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia thì Lĩnh vực y tế là một trong số mười một lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng.

Cục Công nghệ Thông tin đề nghị các đơn vị kiểm tra để kịp thời phát hiện và ngăn chặn cuộc tấn công có chủ đích (nếu có) theo mô tả và hướng dẫn dưới đây.

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 và xoá 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 bytes))

- MD5: BDA82F0D9E2CB7996D2EEFDD1E5B41C4
- SHA-1: 9FF715209D99D2E74E64F9DB894C114A8D13229A

3. Hướng dẫn kiểm tra mã MD5, SHA-1 của tập tin và cách thức xoá tập tin chứa mã độc trong Phụ lục kèm theo.

4. Sau khi thực hiện, đề nghị các đơn vị báo cáo tình hình về Cục Công nghệ thông tin theo địa chỉ email: hotro@moh.gov.vn trước 10h ngày 26/7/2018 để Cục Công nghệ thông tin tổng hợp gửi Cơ quan điều phối sự cố quốc gia theo quy định.

Mọi thông tin chi tiết và đề nghị hỗ trợ kỹ thuật vui lòng liên hệ đầu mối của Trung tâm Tích hợp Dữ liệu: Ông Trần Hoàng Anh – cán bộ kỹ thuật Phòng Hạ tầng và An ninh mạng; email: anhth.cntt@moh.gov.vn; điện thoại: 0986415170.

- Trân trọng./.

Nơi nhận:
- Như trên;
- PCT. Lương Chí Thành (để biết);
- Lưu: VT, THDL.

CỤC TRƯỞNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ Y TẾ

Trần Quý Tường

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: 420 / CNTT-THDL ngày 24 tháng 7 năm 2018 của Cục Công nghệ thông tin)

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 làm bước 2 hướng dẫn gỡ bỏ tệp tin.

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 ta chạy file "procexp.exe".

- 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, ta vào đường dẫn tương ứng để xoá. Kiểm tra các giá trị Registry đã được tạo hoặc thay đổi và xóa.