ỦY BAN NHÂN DÂN **HUYỆN NGA SƠN**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 753 /UBND V/v 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.	*Nga Sơn, ngày 27 tháng 7 năm 2018*

Kính gửi:

- UBND các xã, thị trấn.
- Các cơ quan, đơn vị trên địa bàn huyện.

Thực hiện công văn số 936/STTTT-CNTT ngày 26/7/2018 của Trung tâm Công nghệ Thông tin và Truyền thông Thanh Hóa 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.

Thời gian qua, tình hình mất an toàn thông tin đang diễn biến phức tạp và có chiều hướng gia tăng về tần suất và số lượng các cuộc tấn công xâm nhập vào hệ thống thông tin. Đặc biệt gần đây ghi nhận các hình thức tấn công có chủ đích của tin tặc nhắm vào hệ thống thông tin của một số ngân hàng và hạ tầng quan trọng quốc gia tại Việt Nam. Với hình thức tấn công có chủ đích này, tin tặc đã tìm hiểu kỹ về đối tượng tấn công và thực hiện các thủ thuật lừa đảo, kết hợp các biện pháp kỹ thuật cao để qua mặt các hệ thống bảo vệ an toàn thông tin (ATTT) của các cơ quan, đơn vị nhằm chiếm quyền điều khiển máy tính của người dùng và thông qua đó tấn công các hệ thống thông tin quan trọng khác.

Trên cơ sở công văn số 234/VNCERT-ĐPUC, ngày 21/7/2018 của Trung tâm Ứng cứu sự cố khẩn cấp máy tính Việt Nam (VNCERT). Nhằm tăng cường chủ động kiểm tra, rà soát hệ thống để phòng ngừa, ứng phó và giảm thiểu các sự cố mất an toàn thông tin cho các cơ quan, đơn vị trên địa bàn toàn huyện; Chủ tịch UBND huyện đề nghị Chủ tịch UBND các xã, thị trấn, Thủ trưởng các cơ quan, đơn vị trên địa bàn huyện chỉ đạo các bộ phận liên quan thực hiện tốt một số nội dung sau:

1. Tuyên truyền, phổ biến sâu rộng cho toàn thể cán bộ trong cơ quan, đơn vị về nguy cơ mất an toàn thông tin của hình thức tấn công trên, cũng như khẩn trương nhanh chóng triển khai các biện pháp kỹ thuật để tiến hành rà soát toàn bộ hệ thống thông tin để kịp thời phát hiện và ngăn cuộc tấn công có chủ đích này. Đồng thời tiến hành giám sát và ngăn chặn kết nối đến các máy chủ điều khiển (C&C Server) và rà soát, kiểm tra phát hiện các tệp tin mã độc được tin tặc cài

cắm trong hệ thống thông tin của các cơ quan, đơn vị theo các nội dung hướng dẫn kỹ thuật tại phụ lục kèm theo hoặc được đăng tải trên trang thông tin điện tử của Trung tâm CNTT&TT Thanh Hóa tại địa chỉ: ***http://antoanthongtin.thanhhoaict.gov.vn***

2. Thực hiện nghiêm túc các văn bản chỉ đạo của UBND huyện đã ban hành. Xây dựng phương án để ngăn chặn việc lây lan mã độc trên mạng Truyền số liệu chuyên dùng tại hệ thống mạng của đơn vị.

3. Sau khi thực hiện các biện pháp trên, đề nghị các đơn vị báo cáo kết quả thực hiện về Văn phòng HĐND&UBND huyện trước **14h ngày 30/7/2018** để tổng hợp báo cáo với Sở Thông tin & Truyền thông qua địa chỉ thư điện tử của đ/c Phạm Văn Lưu – cán bộ Văn phòng HĐND & UBND huyện: ***luupv.ngason@thanhhoa.gov.vn***.

Để giúp các cơ quan chức năng theo dõi, phân tích và kịp thời phản ứng nhanh với các phương thức tấn công mới, ngay khi phát hiện sự cố và không có khả năng xử lý, đề nghị các đơn vị thông báo ngay về:

Đầu mối Điều phối ứng cứu sự cố của tỉnh:

Trung tâm Công nghệ thông tin và Truyền thông - Sở Thông tin và Truyền thông Thanh Hóa.

Địa chỉ: 73 Hàng Than, Phường Lam Sơn, TP. Thanh Hóa

Điện thoại: (02373)718.699;

Đường dây nóng: 0916.422.583

Hòm thư điện tử tiếp nhận báo cáo sự cố: ungcuusuco@thanhhoa.gov.vn

Hoặc đ/c Phạm Văn Lưu cán bộ văn phòng HĐND&UBND huyện số điện thoại: 0984.791711.

Đề nghị các cơ quan, đơn vị, UBND các xã, thị trấn quan tâm thực hiện./.

Nơi nhận:
- Sở TTTT; (b/c)
- Như kính gửi;
- Trang thông tin điện tử huyện;
- Đài truyền thanh (đưa tin);
- Lưu: VT, QT.

KT.CHỦ TỊCH
PHÓ CHỦ TỊCH

Mai Đình Hiếu

PHỤ LỤC

HƯỚNG DẪN KIỂM TRA MÃ MD5, SHA-1 CỦA TẬP TIN VÀ CÁCH THỨC XÓA TẬP TIN CHỨA MÃ ĐỘC

(Gửi kèm công văn số: 753/UBND ngày 27 tháng 7 năm 2018 của UBND huyện Nga Sơn)

1. Địa chỉ IP các máy chủ C&C:

a) 38.132.124.250

b) 89.249.65.220

2. Rà quét hệ thống và 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 bytes))

- MD5: BDA82FOD9E2CB7996D2EEFDD 1E5B41C4

- SHA-1: 9FF715209D99D2E74E64F9DB894C114A8D13229A

3. Hướng dẫn kiểm tra mã MD5, SHA-1 của tập tin và cách thức xóa tập tin chứa mã độc

3.1. 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.

3.2. 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.