UỶ BAN NHÂN DÂN **HUYỆN HOẰNG HOÁ**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 605 /UBND - VHTT V/v cảnh báo các phương thức tấn công khai thác hệ thống mới của tin tặc.	*Hoằng Hoá, ngày 15 tháng 5 năm 2017*

Kính gửi:
- Chủ tịch UBND 43 xã, thị trấn;
- Thủ trưởng các cơ quan, đơn vị.

Thực hiện Công văn số 534/STTTT-CNTT ngày 05/5/2017 của Sở Thông tin và Truyền thông V/v các phương thức tấn công khai thác hệ thống mới của nhóm tin tặc Shadow Brockers; UBND huyện đề nghị Chủ tịch UBND các xã, thị trấn, Thủ trưởng các cơ quan, đơn vị quan tâm và thực hiện một số nội dung sau:

1. Theo thông báo của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), nhóm tin tặc có tên gọi Shadow Brockers tuyên bố đã đánh cắp được một bộ công cụ gián điệp có thể khai thác bất kỳ hệ thống thông tin nào sử dụng các phiên bản cũ của hệ điều hành Windows (trừ Windows 10, Windows Server 2016) thông qua các lỗ hổng chưa được khai thác. Nhóm tin tặc đã phát tán bộ công cụ này trên Internet thông qua website chuyên về mã nguồn mở Github. Mục tiêu tấn công của nhóm tin tặc là nhằm vào các tổ chức tiền tệ, ngân hàng lớn, phần đông có trụ sở tại khu vực Trung đông như UAE, Kuwait, Qatar, Palestine và Yemen. Điều này cho thấy nguy cơ mất an toàn thông tin trên diện rộng đa quốc gia, trong đó có Việt Nam.

2. Để giúp việc phòng, tránh các rủi ro mất an toàn thông tin mạng liên quan đến các công cụ tấn công của nhóm tin tặc Shadow Brockers, UBND huyện đề nghị Thủ trưởng các cơ quan, đơn vị thực hiện một số biện pháp sau:

- Tiếp tục phổ biến, quán triệt các văn bản chỉ đạo của Trung ương, của tỉnh và tổ chức triển khai các văn bản hướng dẫn, hỗ trợ kỹ thuật của Sở Thông tin và Truyền thông Thanh Hóa để đảm bảo an toàn thông tin mạng.

- Nhanh chóng rà soát và cập nhật các bản vá lỗi được cảnh báo ở trên tại Website chính thức của Microsoft đối với các máy tính sử dụng hệ điều hành Windows (từ Windows Server 2000 tới Windows Server 2012, Windows XP, Windows Vista, Windows 7, Windows 8,...); cập nhật phiên bản mới nhất của các chương trình diệt Virut để phát hiện và xử lý các mã thực thi do tin tặc tấn công vào hệ thống. Đối với hệ thống mạng sử dụng các thiết bị của Cisco, cập nhật các bản vá lỗi liên quan đến lỗ hổng zero – day (CVE-2016-6366). Để bảo vệ dữ liệu an toàn, máy tính nên được bảo vệ đằng sau Router hoặc Firewalls. Trang bị các hệ thống phòng chống tấn công mạng như IPS/IDS, Firewalls,...

- Thực hiện việc sao lưu dữ liệu định kỳ: Sử dụng các ổ đĩa lưu trữ ngoài như ổ cứng cắm ngoài, ổ đĩa USB để lưu trữ các dữ liệu quan trọng trong máy tính. Sau khi sao lưu xong phải cất giữ riêng và không kết nối vào Internet.

3. Trung tâm CNTT-TT Thanh Hóa là đầu mối tiếp nhận hỗ trợ kỹ thuật, có chức năng xử lý ứng cứu các sự cố liên quan đến dữ liệu, chương trình phần mềm, trang thông tin điện tử, máy tính và mạng nội bộ của các cơ quan, tổ chức đoàn thể

chính trị trên địa bàn tỉnh. Khi các cơ quan, đơn vị gặp các sự cố mà không thể tự khắc phục được, đề nghị liên hệ với Trung tâm CNTT-TT Thanh Hóa để được phối hợp xử lý.

Địa chỉ liên hệ: Trung tâm CNTT-TT Thanh Hóa – 37 Hàng Than - Phường Lam Sơn – TP. Thanh Hóa.

Điện thoại: 0237.3718699 – Fax: 037.3718699.

Địa chỉ Email: ungcuu.sttt@thanhhoa.gov.vn.

Đề nghị Thủ trưởng các cơ quan, đơn vị triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Sở TT&TT (B/c);
- CT, các PCT UBND huyện;
- Các Phòng CM UBND huyện;
- Lưu: VT, VHTT.

KT.CHỦ TỊCH
PHÓ CHỦ TỊCH

Đoàn Thị Hải