UỶ BAN NHÂN DÂN **HUYỆN HOẰNG HOÁ**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 1903/UBND - VHTT V/v ngăn chặn mã độc "đào" tiền ảo.	*Hoằng Hoá, ngày 25 tháng 12 năm 2017*

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

Thực hiện Công văn số 1643/STTTT-CNTT ngày 08/12/2017 của Sở Thông tin và Truyền thông V/v ngăn chặn mã độc "đào" tiền ảo bất hợp pháp; UBND huyện đề nghị Chủ tịch UBND các xã, thị trấn, Thủ trưởng các cơ quan, đơn vị quan tâm thực hiện một số nội dung sau:

1. Theo thông báo của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam: hiện nay, rất nhiều sự cố an toàn thông tin về mã độc khai thác tiền ảo Coinhive ẩn mình trên các trang thông tin điện tử đã được ghi nhận. Khi người dùng truy cập vào trang thông tin điện tử, thư viện mã Coinhive được tự động chạy trên máy tính người dùng dưới dạng tiện ích mở rộng hoặc trực tiếp trong trình duyệt nhằm mục đích "đào" tiền ảo Bitcoin, Monero,... bằng cách sử dụng trái phép tài nguyên người dùng (CPU, ổ cứng, bộ nhớ,...) và gửi về ví điện tử của tin tặc.

Để đảm bảo an toàn thông tin cho các hệ thống thông tin của đơn vị. Thủ trưởng các cơ quan, đơn vị cần thực hiện các nội dung công việc sau:

a. Công tác quản trị cổng/trang thông tin điện tử: Phối hợp với các đơn vị đã xây dựng cổng/trang thông tin điện tử cho cơ quan, đơn vị kiểm tra, rà soát mã nguồn để phát hiện các mã được chèn vào. Dấu hiệu nhận biết gồm các từ khóa trong mã nguồn Website "Coinhive.com", "Coinhive","Coin-hive","Coinhive.min.js", "authedmine.com", "authedmine.min.js".

Nếu phát hiện cổng/trang thông tin điện tử bị chèn các mã khai thác như nêu trên, cần rà soát và kiểm tra lại lỗ hổng trên máy chủ, lỗ hổng trên cổng/trang thông tin điện tử, kiểm tra các tài khoản bị lộ loạt có quyền thay đổi mã nguồn nhằm khắc phục lỗ hổng bị lợi dụng.

b. Công tác quản trị hệ thống mạng nội bộ: Để triển khai các biện pháp nhằm ngăn chặn các đoạn mã trái phép "Coinhive" thực thi trên máy tính của mạng mạng nội bộ, cụ thể như sau:

- Thực hiện giám sát và bóc gỡ, xử lý trên các máy tính trong mạng nội bộ có xuất hiện các kết nối đến các địa chỉ tên miền sau: ajminer.com, Coin-have.com, Coinerra.com, Coinhive.com, Coinnebula.com, crypto-loot.com, hashforcash.com.us, Jescoin.com, ppoi.org, authedmine.min.com.
- Sử dụng tường lửa để ngăn chặn các kết nối ra các địa chỉ sau: afminer.com, Coin-have.com, Coinerra.com, Coinhive.com, Coinnebula.com, crypto-loot.com, hashforcash.us, Jescoin.com, ppoi.orgauthedmine.min.com.
- Rà quét, kiểm tra hệ thống để tìm ra và loại bỏ các đoạn mã có trong các phần mềm mở rộng "Add-on" của trình duyệt web.

- Khuyến nghị người dùng cài đặt các tiện ích mở rộng cho các trình duyệt web: "No Coin Chrome" hay "minerBlock" đối với Chrome; cài đặt "noScripts" cho FireJox.

c. Hướng dẫn người sử dụng kiểm tra hiệu suất sử dụng CPU của máy tính bằng các ứng dụng như Windows Task Manager và Resource Monitor. Nếu máy tính có dấu hiệu chậm chạp và kiểm tra thấy hiệu suất sử dụng CPU của các trình duyệt hoặc tiện ích mở rộng cao thì có thể thấy máy tính đó đã bị nhiễm Coinhive, cần thông báo gấp cho cán bộ quản trị mạng để xử lý.

d. Thường xuyên kiểm tra và quét các lỗ hổng tồn tại trên hệ thống để phát hiện kịp thời sự xuất hiện của các đoạn mã độc hại. Trong trường hợp phát hiện ra các lỗ hổng, lập tức triển khai các biện pháp khắc phục, cập nhật các bản vá bổ sung và loại bỏ các chương trình độc hại đã bị tin tặc chèn vào.

2. Trung tâm CNTT-TT Thanh Hóa là đầu mối tiếp nhận thông tin sự cố, phối hợp hỗ trợ kỹ thuật và xử lý, ứng cứu các sự cố về an toàn thông tin mạng cho các cơ quan, đơn vị trên địa bàn tỉnh.

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: ungcuusuco@thanhhoa.gov.vn.

3. Sau khi thực hiện các biện pháp trên, đề nghị các cơ quan, đơn vị báo cáo tình hình lây nhiễm và kết quả xử lý (nếu có) về UBND huyện (qua Phòng VH-TT) để tổng hợp báo Sở Thông tin và Truyền thông Thanh Hóa theo quy định.

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

Nơi nhận:
- Như trên;
- CT, các PCT UBND huyện;
- Các Phòng CM UBND huyện;
- Lưu: VT, VHTT.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Đoàn Thị Hải