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: 2086/STTTT-CNTT

*Khánh Hòa, ngày 29 tháng 11 năm 2017*

V/v cảnh báo và hướng dẫn ngăn chặn mã độc "đào tiền ảo" bất hợp pháp

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.

Sở Thông tin và Truyền thông nhận được Công văn số 383/VNCERT-ĐPƯC ngày 15/11/2017 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) – Bộ Thông tin và Truyền thông về việc phát hiện, ngăn chặn mã độc "đào tiền ảo" bất hợp pháp.

Theo cảnh báo của Trung tâm VNCERT, qua công tác theo dõi, Trung tâm VNCERT đã ghi nhận được rất nhiều sự cố an toàn thông tin về mã độc khai thác tiền ảo Coinhive ẩn mình trên các cổng/trang thông tin điện tử (website). Mã độc được thực hiện khi người dùng truy cập vào các trang website, 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, Menero… bằng cách sử dụng trái phép tài nguyên người dùng (CPU, ổ cứng, bộ nhớ…) và gửi về ví điện tử của tin tặc.

Do vậy, để chủ động ngăn chặn mã độc trên, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, địa phương khẩn trương thực hiện các nội dung sau:

1. Đối với cán bộ quản trị cổng/trang thông tin điện tử:

- Kiểm tra, rà soát mã nguồn website để phát hiện các mã độc được chèn vào. Dấu hiệu nhận biết gồm các từ khóa trong mã nguồn website như: "coinhive.com", "coinhive", "coin-hive", "coinhive.min.js", "authedmine.com", "authedmine.min.js".

- Nếu phát hiện website bị chèn các mã khai thác như đã nêu trên, cần rà soát và kiểm tra lại lỗ hổng trên máy chủ, lỗ hổng trên websie, kiểm tra các tài khoản bị lộ lọt có quyền thay đổi mã nguồn, nhằm khắc phụ lỗ hổng bị lợi dụng.

- Trường hợp không thể tự thực hiện, các cơ quan có thể đề nghị đơn vị xây dựng cổng/trang thông tin điện tử hỗ trợ thực hiện rà soát, gỡ bỏ mã độc.

2. Đối với cán bộ quản trị mạng, cần triển khai các biện pháp nhằm ngăn chặn việc các đoạn mã trái phép "Coinhive" như sau:

- Thực hiện giám sát và bóc gỡ xử lý trên các máy tính trong mạng có xuất hiện các kết nối đến các địa chỉ tên miền sau: afminer.com, coin-have.com,

coinerra.com, coinhive.com, coinnebula.com, crypto-loot.com, hashforcash.us, jescoin.com, ppoi.org, authedmine.com;

- Hướng dẫn người sử dụng 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 sử dụng cài các tiện ích mở rộng: "No Coin Chrome" hay "minerBlock" đối với trình duyệt Google Chrome; cài đặt "NoScripts" cho trình duyệt Mozilla Firefox.

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

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

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 lây nhiễm 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 ngày 10/12/2017** 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 sự cố mạng máy tính 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/cáo);
- 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: 29.11.2017

**Nguyễn Thị Trung Thu**