UBND HUYỆN LONG ĐIỀN
PHÒNG GIÁO DỤC – ĐÀO TẠO

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

Số: 601 /PGDĐT-VP

Long Điền, ngày 04 tháng 12 năm 2017

V/v phát hiện, ngăn chặn mã độc "đào" tiền ảo bất hợp pháp.

Kính gửi: Hiệu trưởng các trường Mầm non, Tiểu học,
Trung học cơ sở trên địa bàn huyện.

Thực hiện theo Công văn số 2066/SGDĐT-TCCB&CNTT ngày 23/11/2017 của Sở GD&ĐT tỉnh Bà Rịa – Vũng Tàu về việc phát hiện, ngăn chặn mã độc "đào" tiền ảo bất hợp pháp.

Phòng Giáo dục và Đào tạo yêu cầu các đơn vị trường học trên địa bàn huyện thực hiện một số nội dung sau:

1. Phổ biến kiến thức về mã độc "đào" tiền ảo bất hợp pháp: là mã độc khai thác tiền ảo Coinhive ẩn mình trên các website, khi người dùng vào trang web 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.

2. Đối với Quản trị website:

- 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", "authedminc.com", authedmine.min.js, "coinhive", "coin-hive", "coinhive.min.js", "authedmine.com", auihedmine.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 website, kiểm tra các tài khoản bị lộ lọt có quyền thay đổi mã nguồn, nhằm khắc phục lỗ hổng bị lợi dụng.

3. Đối với quản trị mạng: Triển khai các biện pháp nhằm ngăn chặn việc chạy các đoạn mã trái phép "Coinhive" trên máy tính 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: afmincr.com, coin-have.com, coinerra.com, coinhive.com, coinnebula.com. crypto-loot.com, hashforcash.us. jescoin.com, ppoi.org, authcdmine.com;

- Sử dụng tường lửa để chặn các kết nối ra các địa chỉ sau:afminer.com, coin-have.com, coinerra.com, coinhivc.com, coinnebula.com, crypto-loot.com. hashforcash.us, jescoin.com, ppoi.org, authedmine.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: "No Coin Chrome" hay "minerBlock" đối với Chrome; cài đặt "NoScripts" cho Firefox.

- Hướng dẫn người dùng 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 máy tính đó đã bị nhiễm Coinhive cần thông báo gấp cho quản trị mạng để xử lý.

- 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 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.

- Sau khi thực hiện, đề nghị các Đơn vị báo cáo tình hình lây nhiễm và kết quả xử lý (nếu có) trước ngày 10 tháng 12 năm 2017 về Phòng Giáo dục và Đào tạo bằng văn bản để tổng hợp báo cáo về Sở Giáo dục và Đào tạo. Trong quá trình thực hiện nếu có tình huống ứng cứu khẩn cấp xin liên hệ:

+ Trung tâm ứng cứu khẩn cấp máy tinh Việt Nam

Địa chi: Tầng 5 - Tòa nhà 115 Trần Duy Hưng - Cầu Giấy - Hà Nội;

Điện thoại: 04 3640 4423 số máy lẻ 112;

Đường dây nóng: 0869 100 319/0934 424 009;

Hòm thư điện tử tiếp nhận báo cáo sự cố: ir@vncert.gov.vn

Phòng Giáo dục và Đào tạo huyện yêu cầu Hiệu trưởng các trường nghiên cứu và thực hiện đúng nội dung chỉ đạo của Công văn này./.

Nơi nhận:
- Như trên (thực hiện);
- Lưu VT.

KT.TRƯỞNG PHÒNG
PHÓ TRƯỞNG PHÒNG

Digitally signed by Nguyễn Xuân Tiến
Huyện Long Điền
Tỉnh Bà Rịa - Vũng Tàu
Bà Rịa - Vũng Tàu, VN
Date: 4.12.2017 15:0

Nguyễn Xuân Tiến