UBND TỈNH NINH THUẬN
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 4135 /SGDĐT-VP
V/v hướng dẫn rà soát phát hiện, ngăn chặn mã độc khai thác tiền ảo Coinhive bất hợp pháp.

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

Ninh Thuận, ngày 28 tháng 11 năm 2017

Kính gửi:
- Phòng Giáo dục và Đào tạo huyện, thành phố;
- Đơn vị trực thuộc Sở;
- Trưởng các phòng chức năng thuộc Sở.

Tiếp nhận công văn số 1873/STTTT-CNTT ngày 21/11/2017 của Sở Thông tin và Truyền thông về phát hiện, ngăn chặn mã độc "đào" tiền ảo bất hợp pháp;

Hiện nay, Trung tâm VNCERT đã ghi nhận được rất nhiều sự cố ATTT về mã độc khai thác tiền ảo Coinhive ẩn mình trên các website. Khi người dùng truy cập vào website thư viện mã Coinhive được tự động chạy trên máy tính người dùng dưới dạng tiện ích mở rộng hoặc đính trực tiếp trong mã nguồn của 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 phòng ngừa, ngăn chặn việc tấn công của mã độc Coinhive, Sở Giáo dục và Đào tạo cảnh báo và hướng dẫn các đơn vị thực hiện khẩn cấp các việc sau để ngăn chặn tấn công:

1. Đối với các đơn vị có triển khai website riêng:

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", "authedmine.com", authedmine.min.js, "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 website, kiểm tra các tài khoản bị lộ, lọt thông tin truy cập có quyền thay đổi mã nguồn, nhằm khắc phục lỗ hổng bị lợi dụng.

2. Chuyên trách CNTT:

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

- Sử dụng tường lửa để chặn các kết nối ra các địa chỉ sau:afininer.com, coin-have.com, coinerra.com, coinhive.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 bị chèn vào các phần mềm mở rộng "Add-on" của trình duyệt web;

- 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.

3. Đối với người sử dụng:

Có thể chủ động 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 bất thường 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;

Cài đặt các tiện ích mở rộng: "No Coin Chrome" hay "minerBlock" đối với Chrome; cài đặt "NoScripts" cho Firefox.

Chủ động cập nhật các bản vá lỗi, thực hiện các biện pháp khắc phục theo hướng dẫn của quản trị mạng.

4. Đầu mối liên hệ phối hợp xử lý:

Sở Giáo dục và Đào tạo tỉnh Ninh Thuận

- Bà Hoàng Thị Hương Giang, Chuyên viên Văn phòng Sở;

- Điện thoại: 02593.832424;

- Email: hoanggiang@ninhthuan.edu.vn

Sở Thông tin và Truyền thông tỉnh Ninh Thuận

- Ông Quý Minh Phương, Trưởng phòng Công nghệ thông tin

- Điện thoại: 02593.922753;

- Thư điện tử: qmphuong@ninhthuan.gov.vn;

Trung tâm Công nghệ thông tin và Truyền thông

- Ông Võ Trọng Hải, Giám đốc;

- Điện thoại: 02593.838274;

- Email: tronghai@ninhthuan.gov.vn

- Ông Nguyễn Trần Quảng Hà, Chuyên viên quản trị mạng;

- Điện thoại: 02593.838275;

- Email: quangha@ninhthuan.gov.vn

Đề nghị Trưởng phòng Giáo dục và Đào tạo các huyện, thành phố; Các đơn vị trực thuộc Sở; Các phòng chức năng thuộc Sở khẩn trương triển khai các biện pháp trên nhằm phát hiện, ngăn chặn mã độc khai thác tiền ảo bất hợp pháp./.

Nơi nhận:
- Như trên;
- GĐ, PGĐ Sở;
- Cổng TTĐT Ngành;
- Lưu: VT, VP.H.T.H.G.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH NINH THUẬN

Lê Bá Phương