UBND TỈNH HÀ GIANG
SỞ GIAO THÔNG VẬN TẢI

Số: 280/TB-SGTVT
V/v Thông báo phát hiện, ngăn chặn mã độc "đào" tiền ảo bất hợp pháp

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

Hà Giang, ngày 29 tháng 11 năm 2017

Kính gửi: Các Phòng, Ban và các đơn vị trực thuộc.

Ngày 22 tháng 11 năm 2017, Sở Giao thông vận tải nhận được công văn số 608/STTTT-CNTT của sở Thông tin và Truyền thông về việc Thông báo phát hiện, ngăn chặn mã độc "đào" tiền ảo bất hợp pháp. Để đảm bảo an toàn thông tin trong hoạt động của cơ quan nhà nước, đề nghị bộ phận chuyên trách công nghệ thông tin triển khai một số nội dung như sau:

1. Bộ phận chuyên trách công nghệ thông tin (CNTT) có trách nhiệm hướng dẫn, hỗ trợ, các phòng, ban, đơn vị thực hiện việc kiểm tra, rà soát loại bỏ các mã độc trên hệ thống máy tính, khắc phục các sự cố và đảm bảo an toàn, an ninh thông tin trong trong cơ quan.

2. Kiểm tra, rà soát mã nguồn ứng dụng để phát hiện các mã độc được chèn vào.Kiểm tra lỗ hổng trên máy chủ, lỗ hổng website, kiểm tra rà soát các tài khoản và các địa chỉ cá nhân có quyền thay đổi mã nguồn.

Dấu hiện nhận biết bị thiết bị nhiễm mã độc: Mã nguồn Website xuất hiện các từ khóa "coinhive.com", "coinhive", "coin-hive", coinhive.min.js", :authedmine.com", "authedmine.min.js.

3. Triển khai các biện pháp nhằm ngăn chặn việc chạy các đoạn mã độc trái phép "coinhive" trên các máy tính như sau:

- Thực hiện giám sát và gỡ bỏ, xử lý các máy tính trong mạng có xuất hiện các kết nối đến các địa chỉ tên miền sau: afiminer.com, coin-hive.com, coinerra.com. coinhive.com, coinnebula.com, crypto-loot.com, hashforcash.us, jescoin.com, ppoi.org, authedmine.com;

- Sử dụng tường lửa để ngăn chặn các kết nối ra các địa chỉ sau: afminer.com,

Hashforcash.us, jescoin.com, 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 các trình duyệt web;

- Hỗ trợ người dùng cài đặt các tiện ích mở rộng: "No coin Chrome" hay "MinerBlock" đối với Chrome; cài đặt "Noscripts" cho Firefox.

4. 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.

5. Thường xuyên kiểm tra và quét lỗ hổng tồn tại trên các 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 khắc phục bằng cách cập nhật các bản vá bổ sung và loại bỏ các chương trình độc hại.

Trong quá trình triển khai thực hiện các Phòng, ban và các đơn vị gặp sự cố về tấn công khẩn cấp, không giải quyết được phải báo ngay về Văn phòng sở tổng hợp, xin ý kiến và kịp thời tìm cách khắc phục và xử lý.

Đề nghị các Phòng, ban và các đơn vị triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo sở;
- Trang TTĐT;
- Lưu VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ GIAO THÔNG VẬN TẢI
TỈNH HÀ GIANG

Tống Văn Huấn