| | |
|---|---|
| BỘ Y TẾ<br>**CỤC CÔNG NGHỆ THÔNG TIN** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập – Tự do – Hạnh phúc** |
| Số: 629 /CNTT-CSHT<br>V/v phát hiện, ngăn chặn mã độc " đào" tiền ảo bất hợp pháp | *Hà Nội, ngày 15 tháng 12 năm 2017* |

Kính gửi:

- Các Vụ, Cục, Tổng cục, Văn phòng Bộ, Thanh tra Bộ;
- Các đơn vị trực thuộc Bộ Y tế;
- Sở Y tế các tỉnh, thành phố trực thuộc Trung ương.

Ngày 15/11/2017, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam có công văn số 383/VNCERT-ĐPƯC gửi Bộ Y tế về việc phát hiện, ngăn chặn mã độc đào khai thác tiền ảo bất hợp pháp Coinhive ẩn mình trên các website. Khi người dùng truy cập 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,

Căn cứ trên nội dung công văn trên, Cục Công nghệ thông tin đề nghị các đơn vị thực hiện khẩn cấp các công việc sau:

1. 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", "authedmine. corn", authedmine.minj s."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 có quyền thay đổi mã nguồn, nhằm khắc phục lỗ hổng bị lợi dụng.

2. Đối với quản trị mạng: Triển khai các biện pháp nhằm ngăn chặn việc chạy các đoạn mã trái phép "Coinhive" trên các 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.corn, crypto-loot.com, hashforcash.us, jescoin.corn, ppoi.org, authedmine.com;

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

3. Hướng dẫn người dùng kiểm tra hiệu suất sử dụng CPU của máy tính bằng các ứng dụng như Windows Task Manager va 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 roonngj cao thì có thể máy tính đó đã bị nhiễm Coinhive. Cần thông báo gấp cho Quản trị mạng để xử lý

4. 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 lỗ hổng, lập tức triển khai biện pháp khắc phục, cập nhật bản vá bổ sung và loại bỏ các chương trình độc hại đã bị tin tặc chèn vào.

5. Sau khi thực hiện, đề nghị các đơn vị báo cáo tình hình lây nhiễm và kết quả xử lý ( nếu có) về Cục Công nghệ thông tin để phối hợp xử lý.

Xin trân trọng cảm ơn!

***Nơi nhận:***
- Như trên;
- Thứ trưởng Lê Quang Cường (để b/c);
- Cục trưởng (để b/c);
- Lưu: VT, CSHT.

**KT. CỤC TRƯỞNG**
**PHÓ CỤC TRƯỞNG**

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ

**Lương Chí Thành**