BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Số: 383/VNCERT-ĐPƯC
V/v 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 Nội, ngày 15 tháng 11 năm 2017

KHẨN

Kính gửi:
- Các đơn vị chuyên trách về CNTT, ATTT của Văn phòng Trung ương Đảng, các Ban của Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Văn phòng Chính phủ;
- Các đơn vị chuyên trách về CNTT, ATTT các Bộ, ngành;
- Các đơn vị thuộc Bộ Thông tin và Truyền thông;
- Các Sở thông tin và Truyền thông;
- Thành viên mạng lưới ứng cứu sự cố;
- Các Tổng công ty,Tập đoàn Kinh tế, các Tổ chức Tài chính, Ngân hàng;
- Các Doanh nghiệp hạ tầng Internet, Viễn thông, Điện lực, Hàng không, Giao thông Vận tải.

Thực hiện công tác theo dõi sự cố trên không gian mạng Việt Nam, 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 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 Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ và thực hiện Thông tư số 20/2011/TT-BTTTT ban hành ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng toàn quốc, Trung tâm VNCERT yêu cầu Lãnh đạo đơn vị chỉ đạo các đơn vị thuộc phạm vi quản lý 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.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 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 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:afminer.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 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 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.

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 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.

5. Sau khi thực hiện, đề nghị các đơn vị báo cáo tình hình lây nhiễm và kết quả xử lý (nếu có) về Cơ quan Điều phối Quốc gia (Trung tâm VNCERT) trước ngày 30 tháng 11 năm 2017.

Trên đây là loại mã độc nguy hiểm. Trung tâm VNCERT yêu cầu Lãnh đạo các đơn vị nghiêm túc thực hiện lệnh điều phối.

Cơ quan Điều phối Quốc gia:

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam

Địa chỉ: 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.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Giám đốc (để b/c);
- PGĐ Nguyễn Khắc Lịch;
- Các phòng, chi nhánh: KTHT, NCPT, TVĐT, CNHCM, CNĐN;
- Lưu VT, ĐPƯC.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Nguyễn Khắc Lịch