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

Số: 234 /VNCERT-ĐPƯC

V/v theo dõi, ngăn chặn kết nối và xoá các tập tin mã độc tấn công có chủ đích vào ngân hàng và các tổ chức hạ tầng quan trọng quốc gia

HỎA TỐC

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

Hà Nội, ngày 21 tháng 7 năm 2018

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;
- 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.

Trong thời gian gần đây (cuối tháng 7/2018), Trung tâm VNCERT đã ghi nhận các hình thức tấn công có chủ đích của tin tặc nhắm vào hệ thống thông tin của một số ngân hàng và hạ tầng quan trọng quốc gia tại Việt Nam. Với hình thức tấn công có chủ đích này, tin tặc đã tìm hiểu kỹ về đối tượng tấn công và thực hiện các thủ thuật lừa đảo, kết hợp với các biện pháp kỹ thuật cao để qua mặt các hệ thống bảo vệ an toàn thông tin (ATTT) của các ngân hàng và các tổ chức hạ tầng quan trọng nhằm chiếm quyền điều khiển máy tính của người dùng và thông qua đó tấn công các hệ thống máy tính nội bộ chứa thông tin quan trọng khác. Mục đích chính của tin tặc là đánh cắp các thông tin quan trọng của ngân hàng và các tổ chức hạ tầng quan trọng quốc gia. Với việc sử dụng các kỹ thuật cao để tấn công thì các hệ thống bảo vệ ATTT của ngân hàng hoặc các tổ chức hạ tầng quan trọng sẽ khó phát hiện kịp thời và đồng thời giúp tin tặc duy trì quyền kiểm soát hệ thống thông tin.

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc, Trung tâm VNCERT đề nghị các ngân hàng và các tổ chức hạ tầng quan trọng quốc gia thực hiện gấp các biện pháp sau để kịp thời phát hiện và ngăn chặn cuộc tấn công có chủ đích, cụ thể như sau:

1. Theo dõi và ngăn chặn kết nối đến các máy chủ C&C có địa chỉ IP sau:

a) 38.132.124.250

b) 89.249.65.220

2. Rà quét hệ thống và xoá các thư mục và tập tin mã độc có kích thước tương ứng:

a) syschk.ps1 (318 KB (326,224 bytes))

- MD5: 26466867557F84DD4784845280DA1F27

- SHA-1: ED7FCB9023D63CD9367A3A455EC94337BB48628A

b) hs.exe (259 KB (265,216 bytes))

- MD5: BDA82F0D9E2CB7996D2EEFDD1E5B41C4

- SHA-1: 9FF715209D99D2E74E64F9DB894C114A8D13229A

3. Hướng dẫn kiểm tra mã MD5, SHA-1 của tập tin và cách thức xoá tập tin chữa mã độc trong Phụ lục kèm theo.

4. Sau khi thực hiện, yêu cầu các đơn vị báo cáo tình hình về Cơ quan điều phối ứng cứu sự cố quốc gia (Trung tâm VNCERT) theo địa chỉ email: ir@vncert.gov.vn /điện thoại: 0869100319 trước 12h ngày 26/7/2018.

5. Trên đây là những mã độc rất nguy hiểm, có thể đánh cắp thông tin và phá huỷ hệ thống thông tin, Trung tâm VNCERT yêu cầu Lãnh đạo các đơn vị nghiêm túc thực hiện lệnh điều phối.

Trân trọng./.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Nguyễn Khắc Lịch

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 chi nhánh, phòng: CNHCM, CNĐN, KTHT, NCPT, TV&BDNV;
- Lưu VT, ĐPƯC.