BỘ TƯ PHÁP
CỤC CÔNG NGHỆ THÔNG TIN

Số: 105 /CNTT-HTKT&ATTT
V/v phòng tránh các nguy cơ lây nhiễm mã độc.

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

Hà Nội, ngày 25 tháng 3 năm 2019

Kính gửi: - Thủ trưởng các đơn vị thuộc Bộ;
- Cục trưởng Cục thi hành án dân sự các tỉnh, thành phố trực thuộc Trung ương.

Hiện nay, tình hình an toàn an ninh thông tin trong nước đang có diễn biến phức tạp, các đơn vị chuyên trách về an toàn an ninh thông tin liên tục đưa ra các cảnh báo, khuyến nghị về công tác đảm bảo an toàn an ninh thông tin trong giai đoạn hiện nay. Thời gian qua các chuyên gia bảo mật đã phát hiện một loại mã độc có tên gọi **GrandCrab 5.2** và lỗ hổng bảo mật trên phần mềm nén và giải nén tập tin phổ biến **Winrar**.

- Mã độc **GandCrab 5.2** được phát tán thông qua thư điện tử giả mạo từ Bộ Công an Việt Nam với tiêu đề *"Goi trong Cong an Nhan dan Viet Nam"*, có đính kèm tệp tin *documents.rar*. Khi người dùng giải nén và mở tệp tin đính kèm, mã độc sẽ được kích hoạt và toàn bộ dữ liệu người dùng bị mã hóa. Tin tặc khai thác và tấn công sẽ gây lên hậu quả nghiêm trọng.

- Lỗ hổng bảo mật trên phần mềm nén và giải nén **Winrar** cho phép đối tượng tấn công cài đặt mã độc vào máy người dùng và ảnh hưởng đến tất cả các phiên bản của Winrar phát hành trong thời gian qua. Lỗ hổng này có thể được tin tặc lợi dụng để thực hiện tấn công ATP nhằm đánh cắp dữ liệu.

Nhằm bảo đảm an toàn thông tin và phòng tránh nguy cơ bị tấn công bởi mã độc, Cục Công nghệ thông tin đề nghị Thủ trưởng các đơn vị thuộc Bộ, Cục trưởng Cục Thi hành án dân sự các tỉnh, thành phố trực thuộc Trung ương quán triệt cán bộ, công chức, viên chức và người lao động trong đơn vị nâng cao nhận thức, ý thức cảnh giác trong công tác đảm bảo an toàn thông tin và thực hiện nghiêm túc các nội dung sau:

1. Nâng cao cảnh giác, không click vào các liên kết cũng như mở các tập tin đính kèm trong email có chứa các tập tin dạng .doc, .pdf, .zip, rar,... được gửi từ người lạ hoặc nếu email được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường. Và thông báo cho bộ phận chuyên trách quản trị hệ thống hoặc đảm bảo an toàn thông tin khi gặp nghi ngờ.

2. Các đơn vị có hệ thống bảo mật như IDS/IPS, Firewall...cần theo dõi, ngăn chặn kết nối đến các máy chủ điều khiển mã độc tống tiền **GandCrab 5.2** *(www.kakaocorp.link; IP:107.173.49.208)*.

3. Rà soát và kiểm tra phiên bản phần mềm nén và giải nén **Winrar** đang được cài đặt và sử dụng trên toàn bộ máy tính, máy chủ. Máy tính nào đang sử

dụng các phiên bản cũ cần loại bỏ phần mềm khỏi máy tính; Cài đặt, cập nhật lên phiên bản Winrar mới nhất (**Winrar 5.70**). Chú ý chỉ tải phần mềm từ trang chủ Winrar hoặc tổ chức tin cậy. Đường dẫn tải phiên bản Winrar mới nhất: *https:www.win-rar.com/download.html* hoặc *https://www.rarlab.com*.

4. Nghiêm túc thực hiện Quy chế Quản lý, vận hành, khai thác, sử dụng và đảm bảo an toàn thông tin hệ thống mạng máy tính của Bộ Tư pháp (ban hành kèm theo Quyết định số 299/QĐ-BTP ngày 08/02/2014), Quy chế Quản lý, sử dụng Hệ thống thư điện tử của Bộ Tư pháp (ban hành kèm theo Quyết định số 290/QĐ-BTP ngày 12/01/2010) và các quy định về đảm bảo an toàn an ninh thông tin trên môi trường mạng máy tính.

Trong trường hợp cần thiết, Quý đơn vị có thể liên hệ với Phòng Hạ tầng kỹ thuật và An toàn thông tin, số điện thoại: 024.62739717, thư điện tử: *csht@moj.gov.vn* để được hỗ trợ. Thường xuyên cập nhật thông tin về an toàn thông tin tại chuyên mục An toàn thông tin trên trang thông tin điện tử của Cục công nghệ thông tin: *http://cntt.moj.gov.vn*.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Khánh Ngọc (để b/c);
- Lưu: VT.

CỤC TRƯỞNG

CỘNG HÒA XHCN VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ TƯ PHÁP

Nguyễn Tiến Dũng