BM 03/QĐ-TNXL

SỞ Y TẾ THỪA THIÊN HUẾ

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

PHIẾU XỬ LÝ VĂN BẢN ĐẾN

Số đến: 498 Ngày đến 23/12/2019

Cơ quan ban hành văn bản: Cục ATVSTP

Số ký hiệu văn bản: 1064/ATVSTP-TTĐL Ngày tháng văn bản: 20/12/2019

Tham mưu ý kiến xử lý của Văn phòng	Duyệt lãnh đạo	Bộ phận/chuyên viên xử lý văn bản
- KTTT (6) triển khai thực hiện	Ngày:...../...../201..	

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

Số: 104 /CNTT-THDL
V/v nguy cơ bị lây nhiễm mã độc qua lỗ hổng trên phần mềm Winrar chưa cập nhật

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

Hà Nội, ngày 22 tháng 03 năm 2019

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.

(Sau đây gọi tắt là các đơn vị)

Căn cứ Công văn số 251/CATTT-NCSC ngày 18/03/2019 của Cục An toàn Thông tin - Bộ Thông tin và Truyền thông về việc nguy cơ bị lây nhiễm mã độc qua lỗ hổng trên phần mềm Winrar (là phần mềm hỗ trợ nén và giải nén tệp tin) chưa cập nhật. Hiện nay đã có nhiều chiến dịch phát tán mã độc, tấn công mạng thông qua lỗ hổng CVE 2018-20250 trên phần mềm Winrar, lỗ hổng này cho phép đối tượng tấn công cài cắm mã độc vào máy người dùng với hình thức phổ biến như sau:

- Đối tượng tấn công lựa chọn những tệp tin tài liệu có độ tin cậy cao, được nhiều người quan tâm, sau đó chúng sử dụng phần mềm Winrar để nén tệp tin tài liệu này và tệp tin mã độc rồi phát tán tệp tin được nén này bằng cách gửi thư điện tử hoặc gửi trên mạng internet nhưng khi người dùng nhận và mở tệp tin nén này chỉ nhìn thấy tệp tin thông thường (Tham khảo phục lục kèm theo).

- Khi người dùng giải nén tệp tin bằng phần mềm Winrar có chứa lỗ hổng thì mã độc cũng được giải nén vào thư mục Startup của Windows để thực thi trong lần khởi động tiếp theo của máy tính;

Do phần mềm Winrar chưa có cơ chế cập nhật tự động và được dùng phổ biến ở Việt Nam, trong khi nhiều đơn vị chưa chú trọng đến công tác rà soát, kiểm tra đánh giá và xử lý các điểm yếu, lỗ hổng an toàn thông tin. Vì vậy nhằm đảm bảo an toàn thông tin, phòng tránh các nguy cơ lây nhiễm mã độc thông qua lỗ hổng này, Cục Công nghệ thông tin đề nghị các đơn vị thực hiện:

1. Rà soát và kiểm tra phiên bản phần mềm Winrar đang được cài đặt và sử dụng trên các máy tính, máy chủ;

2. Máy tính, máy chủ nào đang sử dụng phần mềm Winrar phiên bản cũ cần loại bỏ phần mềm khỏi máy tính; Cập nhật lên phiên bản phần mềm Winrar mới nhất (hiện tại là Winrar 5.7.0). Chú ý chỉ tải phần mềm từ trang chủ Winrar hoặc tổ chức tin cậy, theo đường dẫn sau: https://www.win-rar.com/download.html hoặc https://www.rarlab.com (tham khảo phụ lục kèm theo).

Mọi thông tin chi tiết và đề nghị hỗ trợ kỹ thuật vui lòng liên hệ đầu mối của Cục Công nghệ thông tin: Ông Hoàng Đăng Trị – Phụ trách Phòng Hạ tầng và An ninh mạng – Trung tâm Tích hợp dữ liệu; email: trihd.cntt@moh.gov.vn; điện thoại: 098 777 2483.

Trân trọng./.

Nơi nhận:
- Như trên;
- Lưu: VT, THDL.

CỤC TRƯỞNG

CỤC CÔNG NGHỆ THÔNG TIN

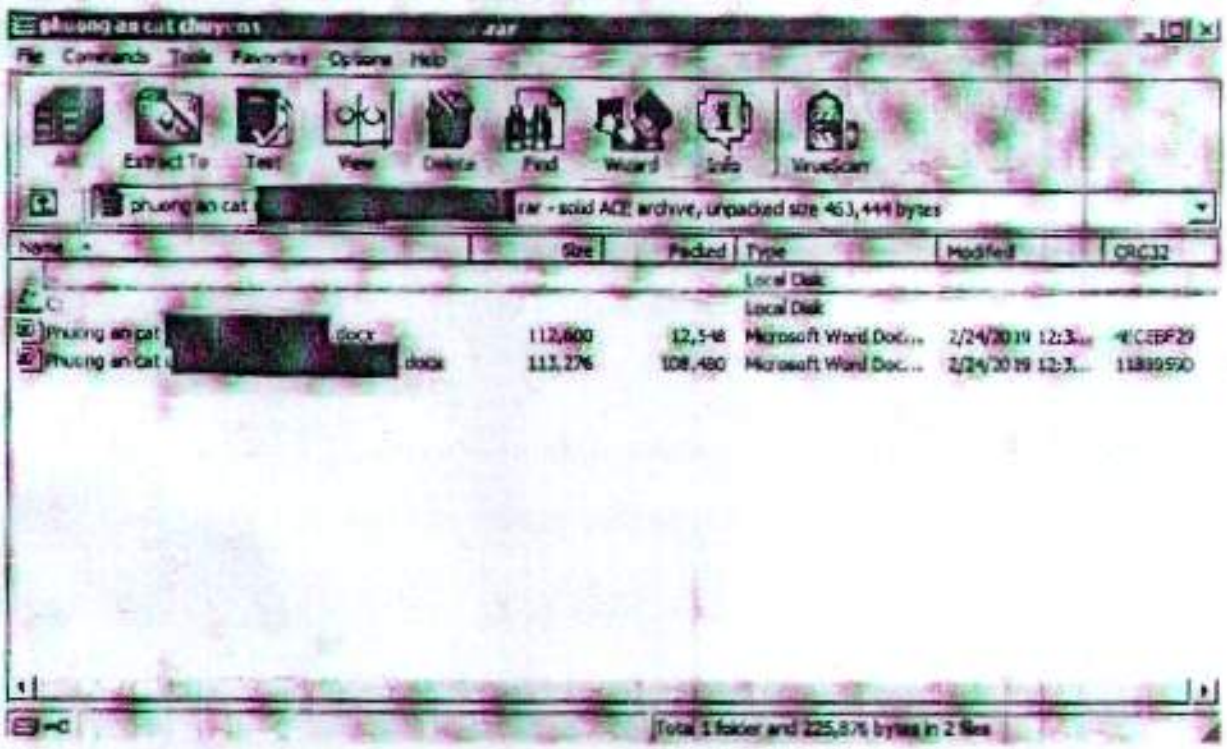
Trần Quý Tường

PHỤ LỤC

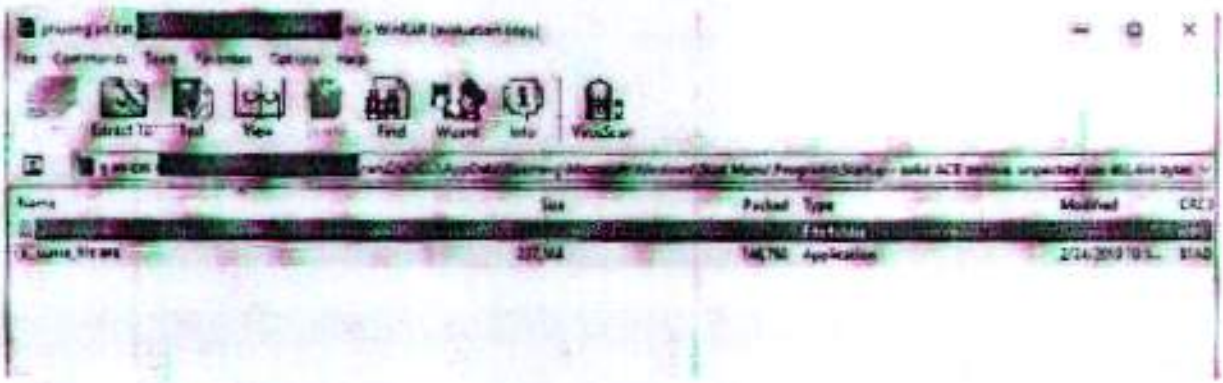
Một số hình ảnh minh họa và hướng dẫn gỡ bỏ, cập nhật phần mềm Winrar

(Kèm theo Công văn số 104 /CNTT-THDL ngày 22 tháng 03 năm 2019)

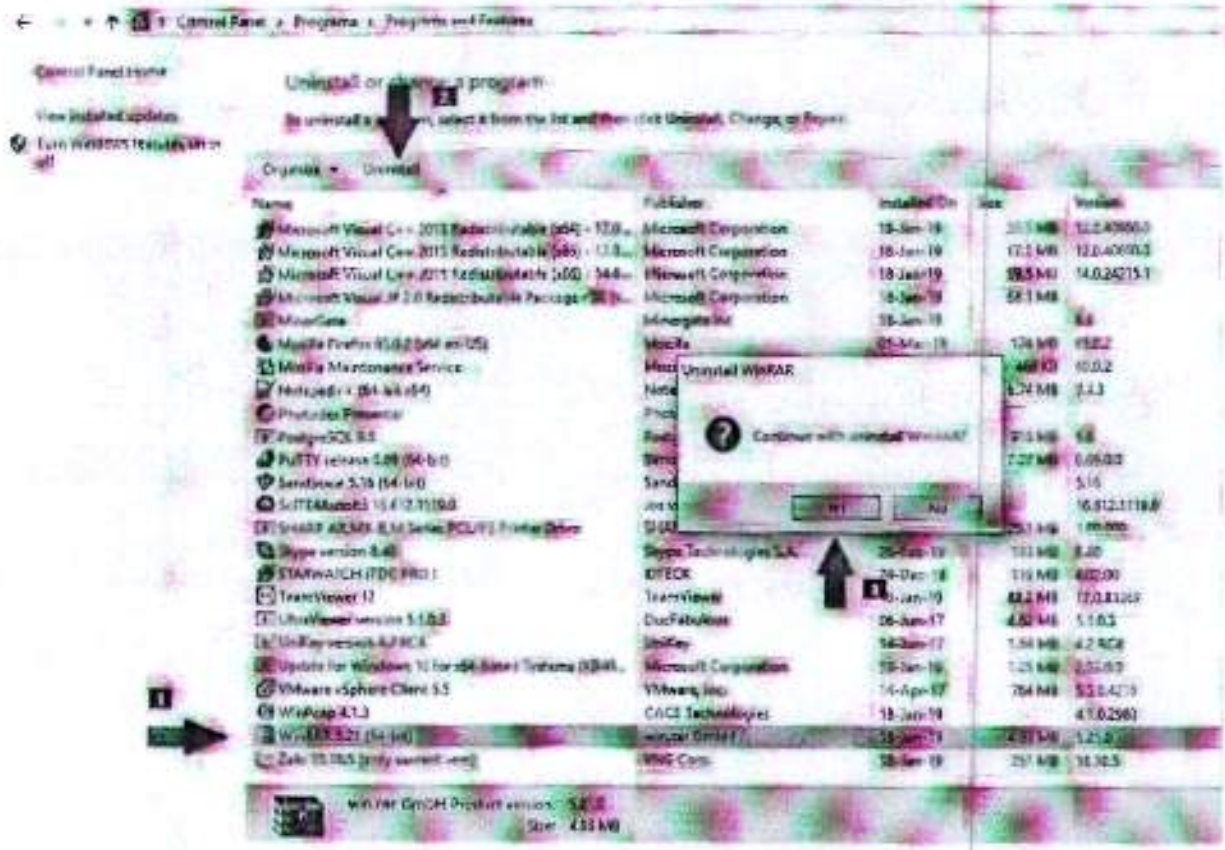
1. Hình ảnh tài liệu nén bằng Winrar được sử dụng để phát tán mã độc



Mã độc được đính kèm vào file nén mà người dùng không biết. Khi giải nén sẽ nằm trong thư mục Startup.



2. Loại bỏ Winrar khỏi máy tính (Hệ điều hành Windows)



3. Tải và cài đặt Winrar từ trang chủ