BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM
CÔNG NGHỆ THÔNG TIN

Số: 63 /TTCNTT-KTHT
V/v nguy cơ 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 21 tháng 03 năm 2019

Kính gửi: Các đơn vị trực thuộc Bộ

Theo thông báo của Cục An toàn thông tin tại Công văn số 251/CATTT-NCSC ngày 18/3/2019, Trung tâm giám sát an toàn thông tin mạng quốc gia (NCSC) thuộc Cục An toàn thông tin đã ghi nhận nhiều chiến dịch phát tán mã độc, tấn công mạng thông qua lỗ hổng trên phần mềm **Winrar (CVE 2018-20250)**. Lỗ hổng này cho phép đối tượng tấn công cài cắm mã độc vào máy người dùng và ảnh hưởng đến tất cả các phiên bản của Winrar phát hành trong thời gian qua. Hình thức phổ biến để phát tán mã độc được đối tượng tấn công đã thực hiện như sau:

- Lựa chọn những tập tin tài liệu có độ tin cậy cao, thường sử dụng tài liệu của chương trình, hội nghị được nhiều người quan tâm;
- Sử dụng phần mềm Winrar để nén tập tin tài liệu này và tập tin mã độc. Phát tán tập tin nén bằng phần mềm Winrar qua nhiều kênh khác nhau: thư điện tử, hoặc các tập tin tài liệu trên mạng (tài liệu hội nghị, hội thảo...). Người dùng mở tập tin nén này sẽ chỉ nhìn thấy tập tin tài liệu thông thường.
- Khi người dùng giải nén 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.

Trước thực trạng trên cùng với việc Winrar là một trong những phần mềm nén tập tin phổ biến ở Việt Nam nhưng chưa có cơ chế cập nhật tự động, đồng thời nhiều cơ quan tổ chức chưa chú trọng đến công tác rà soát, xử lý các điểm yếu lỗ hổng ATTT. Vì vậy, nhằm bảo đảm an toàn thông tin, phòng tránh các nguy cơ lây nhiễm mã độc thông qua lỗ hổng này, Trung tâm 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 toàn bộ máy tính, máy chủ;

2. Máy tính nào đang sử dụng các phiên bản cũ cần loại bỏ phần mềm khỏi máy tính; Cập nhật lên phiên bản Winrar mới nhất (Winrar 5.7.0). 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 (Tham khảo *hướng dẫn kèm theo*).

Trong trường hợp cần thiết xin vui lòng liên hệ Phòng Kỹ thuật hạ tầng – Trung tâm Công nghệ thông tin, số điện thoại: 024.39439060, thư điện tử phongktht@most.gov.vn để được hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Lưu: TTCNTT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

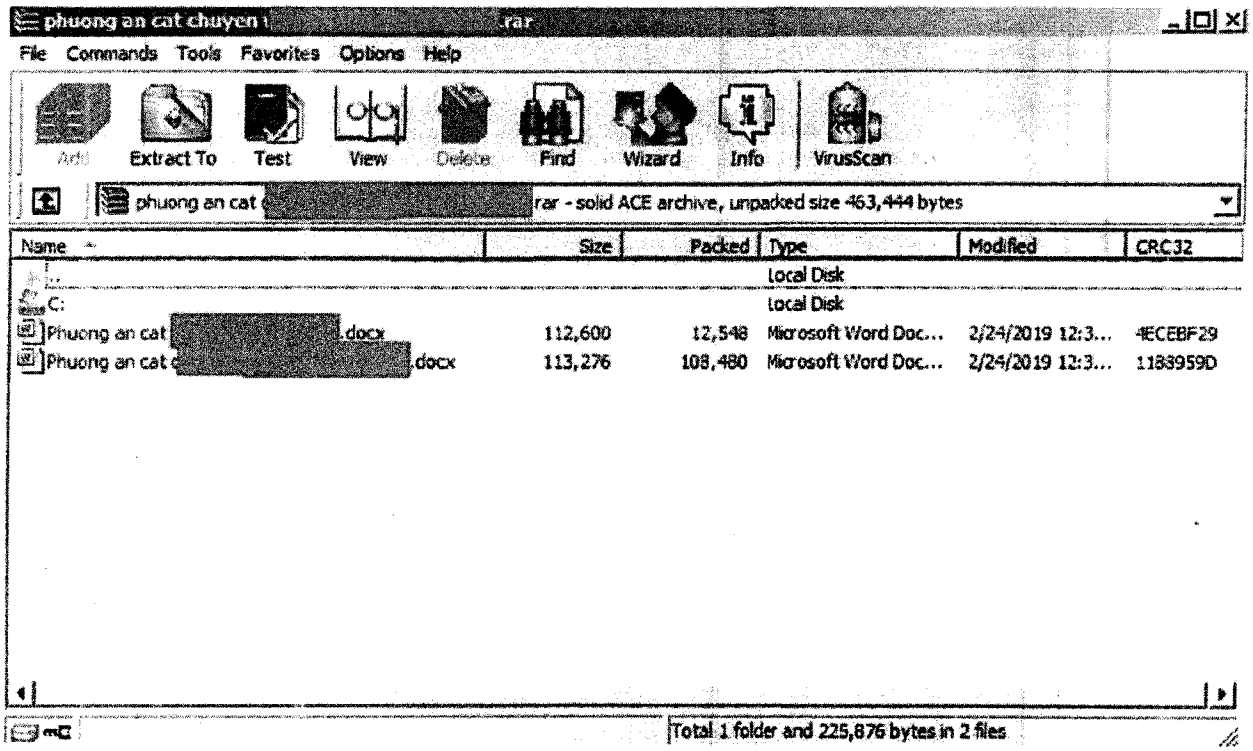
PHỤC LỤC

Một số hình ảnh minh hoạ và hướng dẫn gỡ bỏ, cập nhật

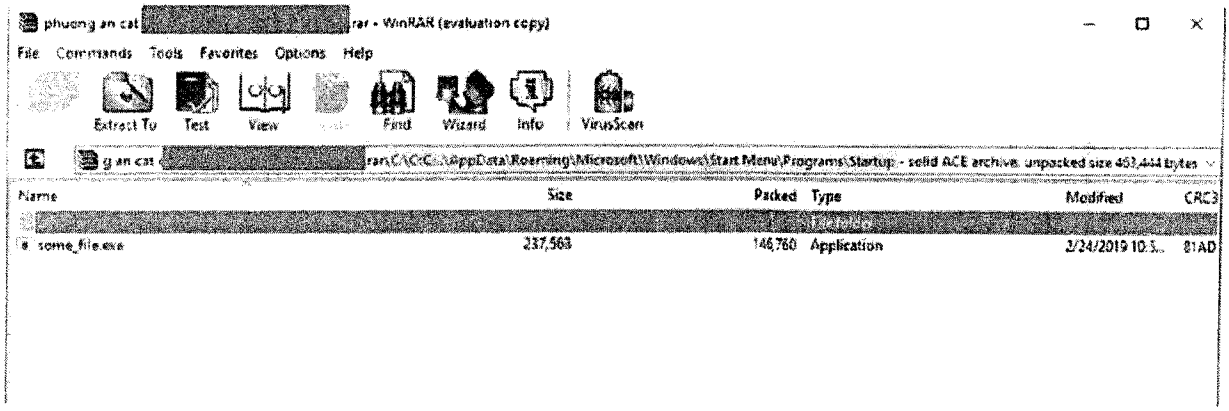
(Kèm theo Công văn số 63 /TTCNTT-KTHT ngày 21 /03/2019 của Trung tâm Công nghệ thông tin)

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

- Hình ảnh khi người dùng sử dụng phần mềm Winrar để nén các tập tin tài liệu

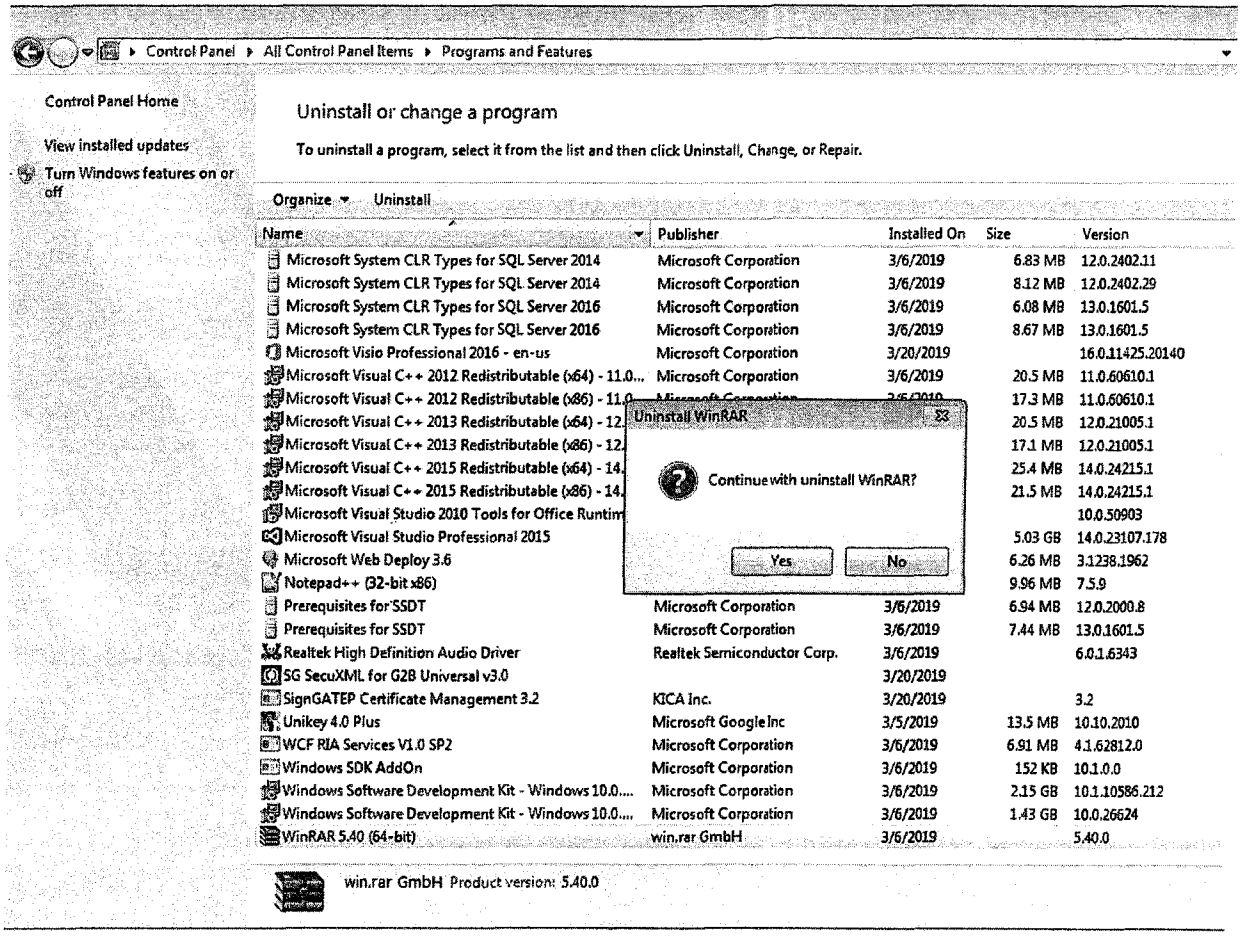


- Hình ảnh sau khi người dùng giải nén file và Mã độc được đính kèm trong file nén mà người dùng không biết. Sau khi giải nén mã độc sẽ nằm trong thư mục Startup



2. Loại bỏ Winrar khỏi máy tính (hệ điều hành windows)

Vào Start => Control Panel => All Control Panel Items => Programs and Features => WinRAR … => Uninstall => Yes.



3. Tải và cài đặt Winrar từ trang chủ (tương ứng với hệ điều hành)

If you don't know what you are looking for then you are probably looking for this:

WinRAR 5.70 64bit

Download WinRAR

If you are looking for the 32bit version click here, or did not find what you were looking for, please search below...

Select for download

Language All Version All Platform All Arch-Type All Search

Language	Version	Size	Arch-Type	Platform
English	5.70	3068 KB	64bit	Windows
English	5.70	2863 KB	32bit	Windows