BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 251/CATTT-NCSC
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 18 tháng 03 năm 2019

Kính gửi:

- Đơn vị chuyên trách về CNTT các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; Các Ngân hàng TMCP; Các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Thời gian gần đây, Trung tâm Giám sát an toàn thông tin mạng quốc gia (NCSC) thuộc Cục An toàn thông tin (Cục ATTT) 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 (Tham khảo *hình ảnh kèm theo*);

- 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.

Đặc biệt lỗ hổng này cũng đã được lợi dụng để thực hiện tấn công APT trong sự kiện Hội nghị thượng đỉnh Hoa Kỳ - Triều Tiên để tấn công vào một số cơ quan tổ chức Việt Nam thực hiên các công tác tổ chức cho sự kiện. Cục ATTT đã cảnh báo nguy cơ tấn công mạng bằng lỗ hổng này thông qua Hệ

thống phân tích và chia sẻ nguy cơ tấn công mạng Việt Nam (https://ti.khonggianmang.vn), Bản tin ATTT Tuần 7, Tuần 9/2019.

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, Cục ATTT đề nghị các cơ quan, tổ chức, doanh nghiệp 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, Quý đơn vị có thể liên hệ với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), số điện thoại: 0243.209.1616, thư điện tử ais@mic.gov.vn để được hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Trung tâm VNCERT;
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HOÀ X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

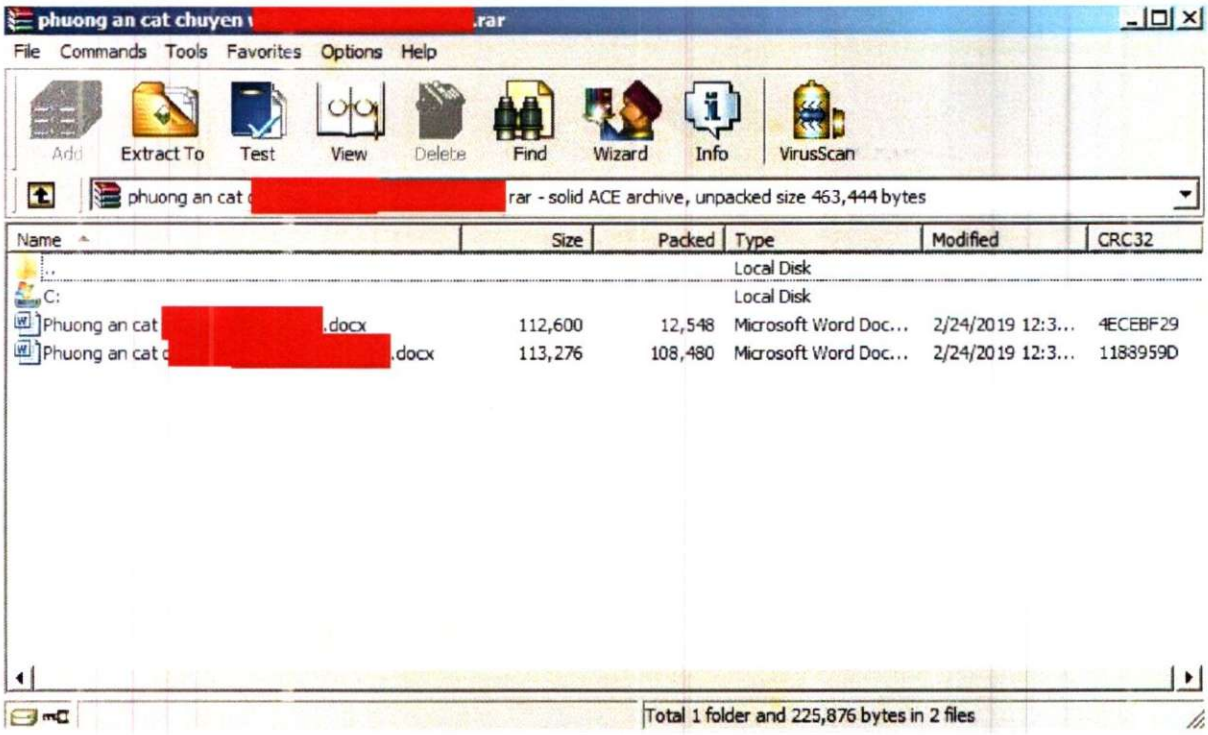
Nguyễn Huy Dũng

Phụ lục

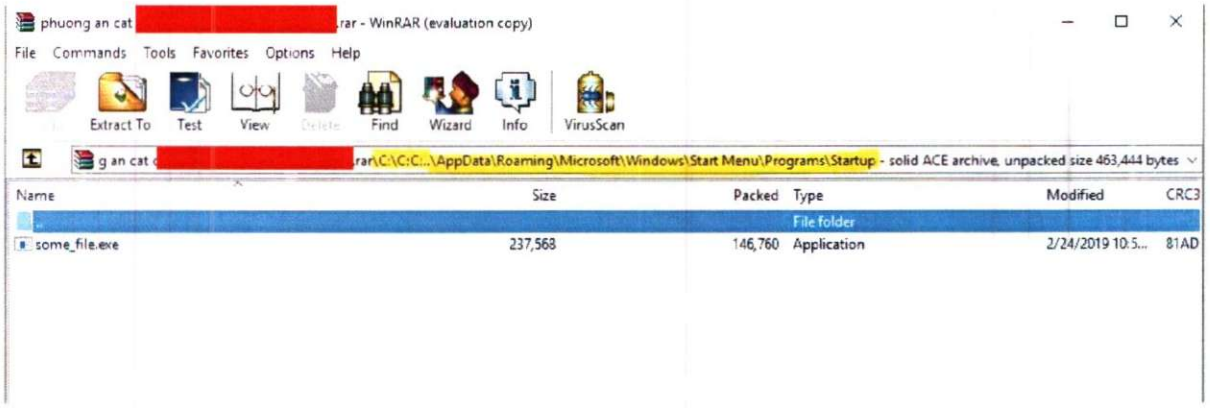
Một số hình ảnh minh hoạ và hướng dẫn gỡ bỏ, cập nhật

(Kèm theo Công văn số 251/CATTT-NCSC ngày 18/3/2019)

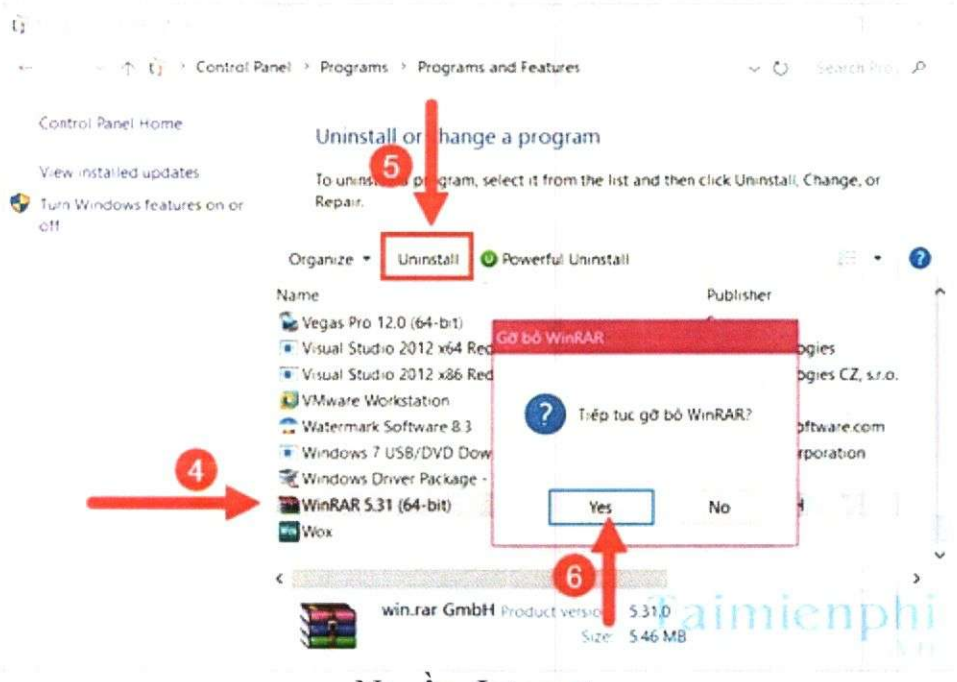
1. Hình ảnh tài liệu nén bằng Winrar được sử dụng để phát tán mã độc



Mã độc được đính kèm trong 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)



Nguồn: Internet

3. Tải và cài đặt Winrar từ trang chủ

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
Arabic	5.70	3110 KB	64bit	Windows
Armenian	5.70	3111 KB	64bit	Windows