

Số: 104 /CNTT-THDL

Hà Nội, ngày 22 tháng 03 năm 2019

V/v nguy cơ bị lây nhiễm mã độc
qua lỗ hổng trên phần mềm
Winrar chưa cập nhật

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 phức 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.winrar.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

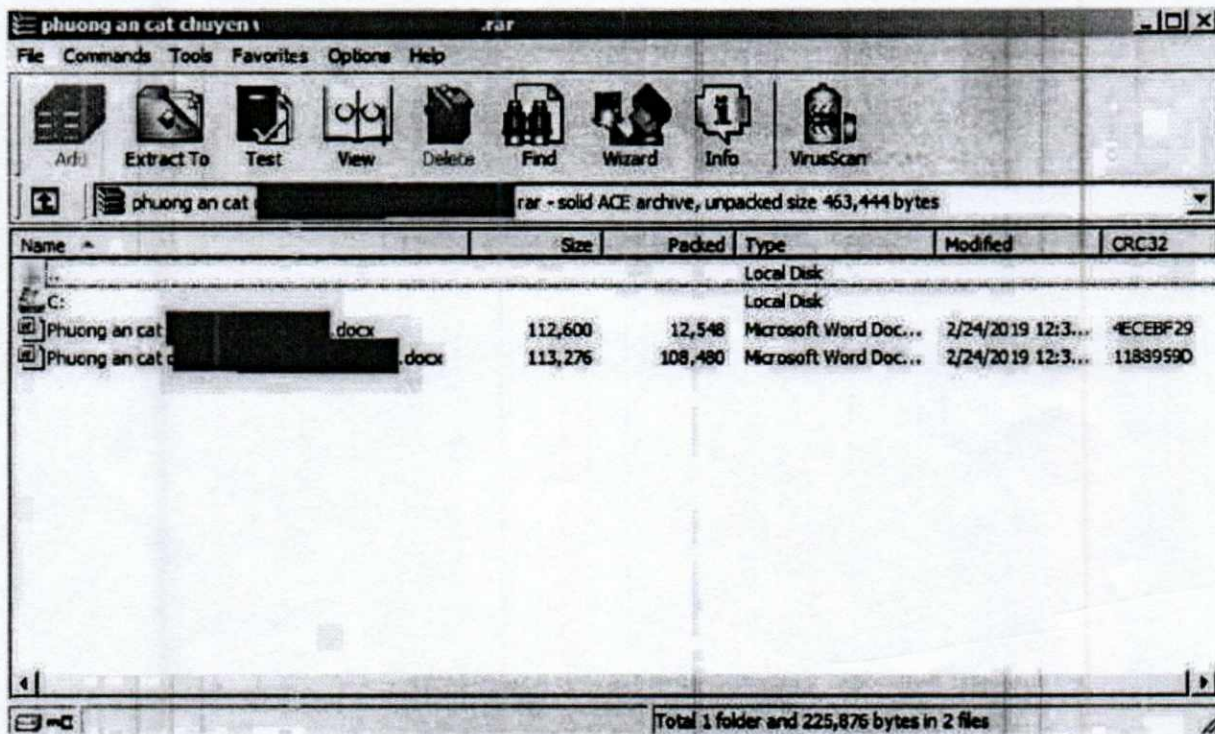
Trần Quý Tường

PHỤ LỤC

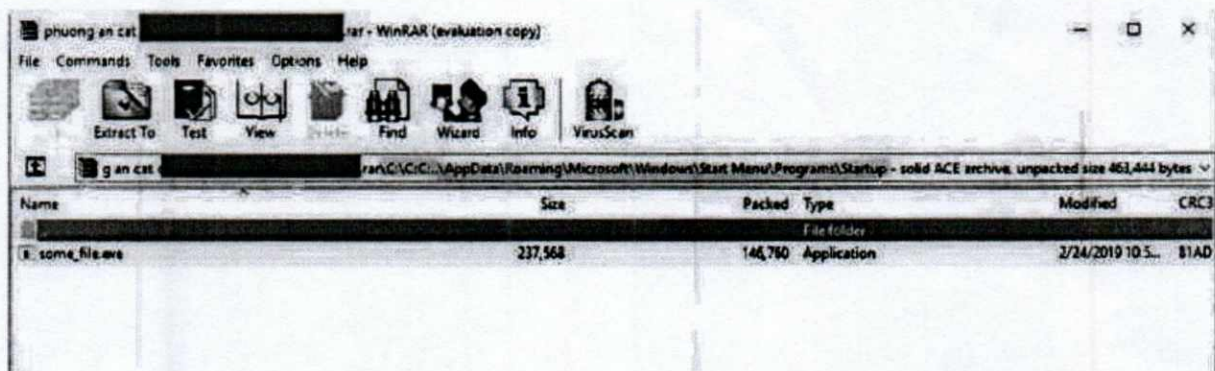
Một số hình ảnh minh họa và hướng dẫn gỡ bỏ, cập nhật phần mềm Winrar

(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)

Control Panel Home

View installed updates

Turn Windows features on or off

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Organize Uninstall

Name	Publisher	Installed On	Size	Version
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0...	Microsoft Corporation	18-Jan-19	20.5 MB	12.0.40660.0
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0...	Microsoft Corporation	18-Jan-19	17.1 MB	12.0.40660.0
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0...	Microsoft Corporation	18-Jan-19	19.5 MB	14.0.24215.1
Microsoft Visual J# 2.0 Redistributable Package - SE (x...	Microsoft Corporation	18-Jan-19	68.1 MB	
MinerGate	Minergate Inc	18-Jan-19		6.9
Mozilla Firefox 65.0.2 (x64 en-US)	Mozilla	01-Mar-19	174 MB	65.0.2
Mozilla Maintenance Service	Mozilla		469 KB	60.0.2
Notepad++ (64-bit x64)	Notepad++		6.74 MB	7.3.3
Photodex Presenter	Photodex		915 MB	9.6
PostgreSQL 9.6	PostgreSQL		7.07 MB	0.69.0.0
PutTY release 0.69 (64-bit)	Simon			5.16
Sandboxie 5.16 (64-bit)	Sandboxie			16.612.1119.0
SciTE4AutoIt3 16.612.1119.0	SciTE4AutoIt3			1.00.000
SHARP AR-MX-B,M Series PCL/PS Printer Driver	SHARP		29.1 MB	8.40
Skype version 8.40	Skype Technologies S.A.	28-Feb-19	193 MB	8.40.00
STARWATCH ITDC PRO I	IDTECK	24-Dec-18	119 MB	4.02.00
TeamViewer 12	TeamViewer	18-Jan-19	88.2 MB	12.0.83369
UltraViewer version 5.1.0.3	DucFabulous	06-Jun-17	4.62 MB	5.1.0.3
UniKey version 4.2 RC4	UniKey	14-Jun-17	1.64 MB	4.2 RC4
Update for Windows 10 for x64-based Systems (KB40...	Microsoft Corporation	18-Jan-19	1.05 MB	2.53.0.0
VMware vSphere Client 5.5	VMware, Inc.	14-Apr-17	764 MB	5.5.0.4216
WinPcap 4.1.3	CACE Technologies	18-Jan-19		4.1.0.2980
WinRAR 5.21 (64-bit)	win.rar GmbH	18-Jan-19	4.93 MB	5.21.0
Zalo 18.10.5 (only current user)	VNG Corp.	18-Jan-19	261 MB	18.10.5

win.rar GmbH Product version: 5.21.0
Size: 4.93 MB

Uninstall WinRAR

Continue with uninstall WinRAR?

Yes No

3. Tải và cài đặt Winrar từ trang chủ

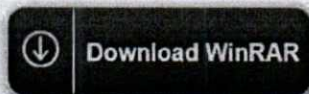
RARLAB® WinRAR®

Search enter your search term here

Language English

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

[WinRAR 5.70 64bit](#)



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