

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: 21/3/2019Cơ quan ban hành văn bản: Cục CNTT
Số ký hiệu văn bản: 104/CNV.T - TT.DL Ngày tháng văn bản: 21/3/2019

Tham mưu ý kiến xử lý của Văn phòng	Duyệt lãnh đạo	Bộ phận/chuyên viên xử lý văn bản
<p>- CNTT (6) - liên khai thực hiện</p>	<p><u>mm</u></p> <p>Ngày:/...../201...</p>	

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

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.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 Trí – 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.



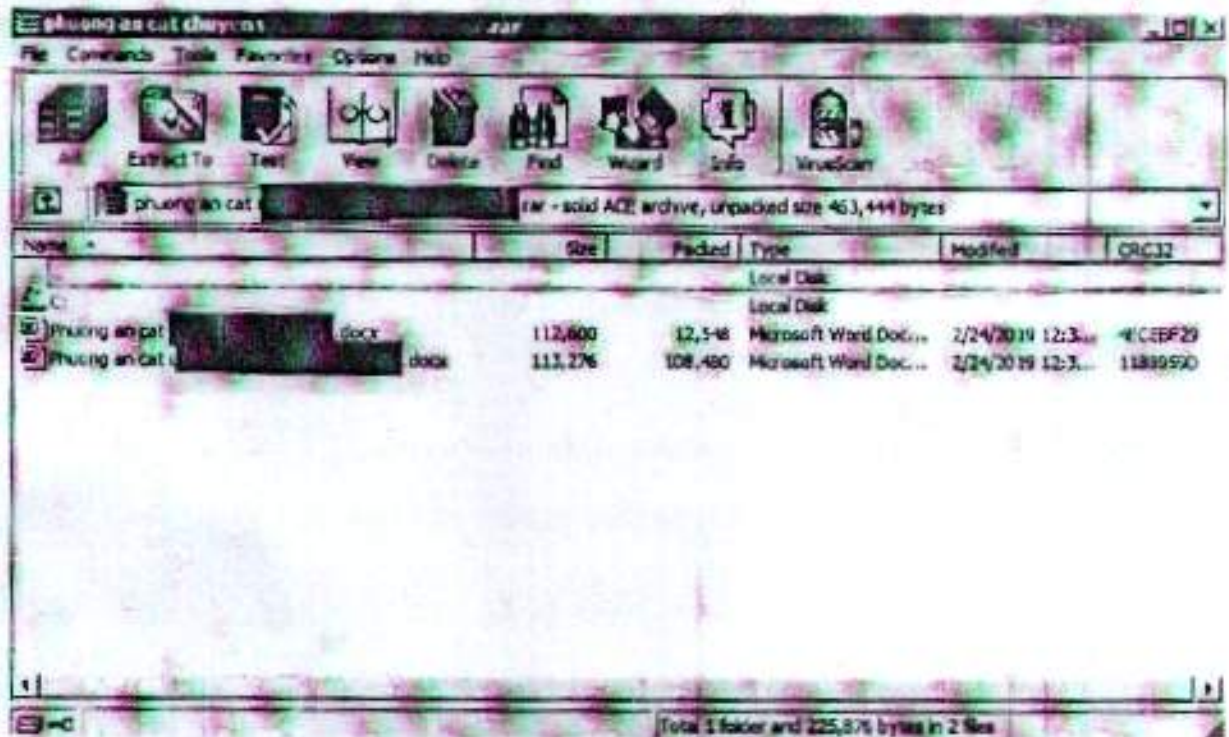
Trần Quý Tường

PHỤ LỤC

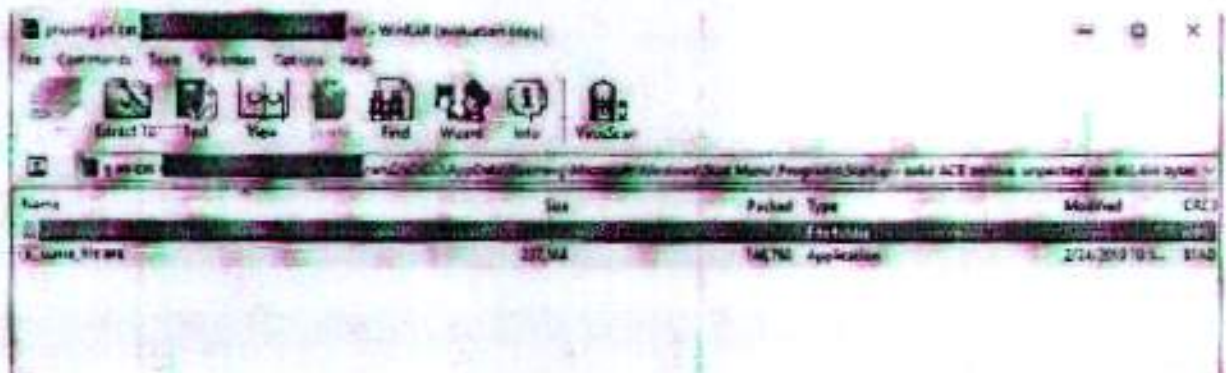
Một số hình ảnh minh họa và hướng dẫn gỡ bỏ, cập nhật phần mềm Winrar

(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 > Programs > Programs and Features

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.

Organization: Uninstall

Name	Publisher	Installed On	Size	Version
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0....	Microsoft Corporation	18-Jan-19	20.5 MB	12.0.49586.0
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0...	Microsoft Corporation	18-Jan-19	17.5 MB	12.0.49586.0
Microsoft Visual C++ 2011 Redistributable (x64) - 11.0...	Microsoft Corporation	18-Jan-19	39.5 MB	11.0.6095.9
Microsoft Visual C++ 2011 Redistributable (x86) - 11.0...	Microsoft Corporation	18-Jan-19	39.1 MB	11.0.6095.9
MiniGate	Minigate Ltd	18-Jan-19	8.8	8.8
Mobile Center (5.6.2) (64-bit) (US)	Motorola	01-Mar-19	128 MB	5.6.2
Media Management Service	Microsoft Corporation	18-Jan-19	468 KB	6.0.0.2
NetSetup (1.0.0) (x64)	Microsoft Corporation	18-Jan-19	1.24 MB	1.1.1
Proxifier Personal	Proxifier Ltd	18-Jan-19	7.1 MB	6.8
SQL Server 2012	Microsoft Corporation	18-Jan-19	7.27 MB	11.0.5424.1
PUTTY (release 0.76) (64-bit)	Simon St Laurent	18-Jan-19	516	0.76.0.3
Sendmail 5.79 (64-bit)	Sendmail, Inc.	18-Jan-19	16,812,118 MB	5.79
SQLite (3.8.11) (64-bit)	SQLite.org	18-Jan-19	251 KB	3.8.11.0
SQL Server 2012 R2 (64-bit) (x64) (English) (Developer)	Microsoft Corporation	18-Jan-19	103 MB	11.0.5424.1
Stype version 8.4.0	Stype Technologies S.A.	26-Feb-19	119 MB	8.4.0
STARWATCH (PDF) PRO 1	STRECK	28-Dec-18	119 MB	6.02.00
TeamViewer 11	TeamViewer	01-Jan-19	82.2 MB	11.0.1310.0
UltraViewer version 5.1.0.3	DuoFabulous	26-Jun-17	4.82 MB	5.1.0.3
UnRAR version 6.07 RC4	RARLAB	18-Jan-19	1.54 MB	4.2 RC4
Update for Windows 10 for x64-based Systems (KB4470418)	Microsoft Corporation	19-Jan-19	1.25 MB	10.0.17134.1
VMware vSphere Client 5.5	VMware, Inc.	14-Apr-07	784 MB	5.5.4.7.9
WinAmp 4.7.1	GNOME Technologies	18-Jan-19	4.91 MB	4.7.0.2961
WinRAR 5.71 (64-bit)	RARLAB	18-Jan-19	4.91 MB	5.71.0
Zulu 75.0.0 (only server-side)	Oracle Corp.	18-Jan-19	29.1 MB	75.0.0

WinRAR (RARLAB) Product version: 5.71.0 Size: 4.91 MB

3. Tải và cài đặt Winrar từ trang chủ

RARLAB® WinRAR®

Search

Language:

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: Version: Platform: Arch-Type:

Language	Version	Size	Arch-Type	Platform
English	5.70	3568 KB	64bit	Windows
English	5.70	2863 KB	32bit	Windows