

Số: 63 /TTCNTT-KTHT

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

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:

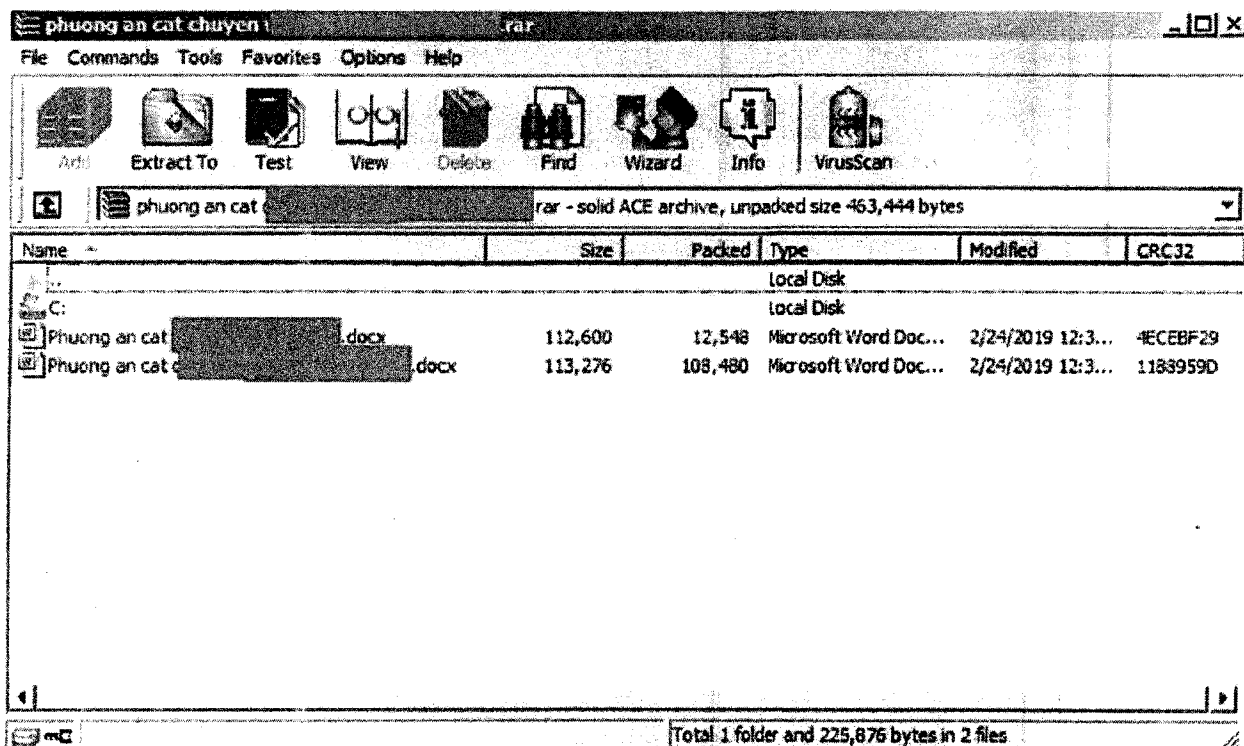
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Lưu: TTCNTT.



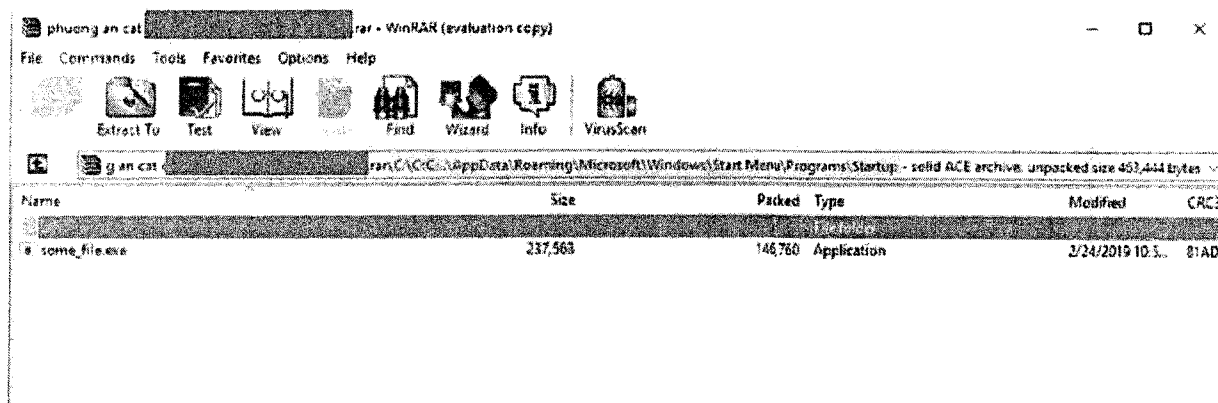
PHỤC LỤC

Một số hình ảnh minh họa 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.

Control Panel > All Control Panel Items > Programs and Features

Control Panel Home

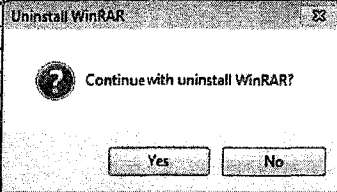
Uninstall or change a program

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 System CLR Types for SQL Server 2014	Microsoft Corporation	3/6/2019	6.83 MB	12.0.2402.11
Microsoft System CLR Types for SQL Server 2014	Microsoft Corporation	3/6/2019	8.12 MB	12.0.2402.29
Microsoft System CLR Types for SQL Server 2016	Microsoft Corporation	3/6/2019	6.08 MB	13.0.1601.5
Microsoft System CLR Types for SQL Server 2016	Microsoft Corporation	3/6/2019	8.67 MB	13.0.1601.5
Microsoft Visio Professional 2016 - en-us	Microsoft Corporation	3/20/2019		16.0.11425.20140
Microsoft Visual C++ 2012 Redistributable (x64) - 11.0...	Microsoft Corporation	3/6/2019	20.5 MB	11.0.60610.1
Microsoft Visual C++ 2012 Redistributable (x86) - 11.0...	Microsoft Corporation	3/6/2019	17.3 MB	11.0.60610.1
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0...	Microsoft Corporation	3/6/2019	20.5 MB	12.0.21005.1
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0...	Microsoft Corporation	3/6/2019	17.1 MB	12.0.21005.1
Microsoft Visual C++ 2015 Redistributable (x64) - 14.0...	Microsoft Corporation	3/6/2019	25.4 MB	14.0.24215.1
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0...	Microsoft Corporation	3/6/2019	21.5 MB	14.0.24215.1
Microsoft Visual Studio 2010 Tools for Office Runtime	Microsoft Corporation	3/6/2019		10.0.50903
Microsoft Visual Studio Professional 2015	Microsoft Corporation	3/6/2019	5.03 GB	14.0.23107.178
Microsoft Web Deploy 3.6	Microsoft Corporation	3/6/2019	6.26 MB	3.1238.1962
Notepad++ (32-bit x86)	Notepad++	3/6/2019	9.96 MB	7.5.9
Prerequisites for SSDT	Microsoft Corporation	3/6/2019	6.94 MB	12.0.2000.8
Prerequisites for SSDT	Microsoft Corporation	3/6/2019	7.44 MB	13.0.1601.5
Realtek High Definition Audio Driver	Realtek Semiconductor Corp.	3/6/2019		6.0.1.6343
SG SecuXML for G2B Universal v3.0	SG SecuXML	3/20/2019		
SignGATEP Certificate Management 3.2	KICA Inc.	3/20/2019		3.2
Unikey 4.0 Plus	Microsoft Google Inc	3/5/2019	13.5 MB	10.10.2010
WCF RIA Services V1.0 SP2	Microsoft Corporation	3/6/2019	6.81 MB	4.1.62812.0
Windows SDK AddOn	Microsoft Corporation	3/6/2019	152 KB	10.1.0.0
Windows Software Development Kit - Windows 10.0...	Microsoft Corporation	3/6/2019	2.15 GB	10.1.10586.212
Windows Software Development Kit - Windows 10.0...	Microsoft Corporation	3/6/2019	1.43 GB	10.0.26624
WinRAR 5.40 (64-bit)	win.rar GmbH	3/6/2019		5.40.0

win.rar GmbH Product version: 5.40.0



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



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	3068 KB	64bit	Windows
English	5.70	2863 KB	32bit	Windows