UBND THÀNH PHỐ HẢI PHÒNG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2648 /STTTT-CNTT
V/v đảm bảo an toàn thông tin trong sử dụng dịch vụ chữ ký số chuyên dùng Chính phủ

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hải Phòng, ngày 25 tháng 12 năm 2020

Kính gửi:
- Các Sở, ban, ngành thành phố;
- Các cơ quan Trung ương tổ chức theo ngành dọc;
- Ủy ban nhân dân các quận, huyện.

Ngày 16/12/2020, Cục Chứng thư số và Bảo mật thông tin, Ban Cơ yếu Chính phủ có công văn số 458/CTSBMTT-QTHT về việc đảm bảo an toàn thông tin trong sử dụng dịch vụ chữ ký số chuyên dùng Chính phủ *(gửi kèm văn bản)*.

Để đảm bảo an toàn thông tin cho các hoạt động ứng dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ, Sở Thông tin và Truyền thông trân trọng đề nghị các cơ quan, đơn vị thực hiện:

- Phổ biến đến các cán bộ, công chức, viên chức, người lao động trong đơn vị nâng cao nhận thức về an toàn thông tin mạng nói chung và cảnh giác với các nguy cơ tấn công mạng có chủ đích nói riêng.

- Thường xuyên thực hiện đánh giá, rà quét mã độc các máy tính của cơ quan, đơn vị. Triển khai cài đặt phần mềm quét virus có bản quyền. Các đơn vị không cài đặt phần mềm quét virus có bản quyền, có thể tải công cụ được Cục Chứng thư số và Bảo mật thông tin cấp để kiểm tra, rà quét mã độc tại địa chỉ: http://av.bcy.gov.vn.

- Thực hiện theo hướng dẫn đảm bảo an toàn thông tin trong sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ của Cục Chứng thư số và Bảo mật thông tin *(gửi kèm theo)* tại địa chỉ: https://ca.gov.vn.

- Phổ biến, hướng dẫn thực hiện các nội dung trên tới 100% các đơn vị trực thuộc.

Sở Thông tin và Truyền thông cử ông Nguyễn Đông Huy (Trưởng Phòng Hạ tầng kỹ thuật và An toàn thông tin - Trung tâm Thông tin và Truyền thông, số điện thoại 098.4462472) là đầu mối phối hợp, trao đổi thông tin.

Trân trọng./.

Nơi nhận:
- Như trên;
- UBNDTP (để b/c);
- Ban 114 (để b/c);
- GĐ, các PGĐ Sở;
- TT TT&TT;
- Cổng TTĐT Sở, Cổng Tin tức TP;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
THÀNH PHỐ HẢI PHÒNG

Lê Văn Kiên

Hướng dẫn đảm bảo an toàn thông tin cho người dùng sử dụng chữ ký số Chuyên dùng Chính phủ *(tại địa chỉ: https://dvc.ca.gov.vn/-/huong-dan-am-bao-an-toan-thong-tin-cho-nguoi-dung-su-dung-chu-ky-so-chuyen-dung-chinh-phu)*

(Thứ năm, 17/12/2020 18:32)

Trong thời gian gần đây thông qua hệ thống theo dõi, giám sát và phân tích mã độc của Trung tâm CNTT và Giám sát An ninh mạng - Ban Cơ yếu Chính phủ đã phát hiện nhiều chiến dịch tấn công có chủ đích sử dụng mã độc vào máy tính người dùng tại các cơ quan Đảng và Nhà nước, trong đó có các máy tính sử dụng chữ ký số chuyên dùng Chính phủ phục vụ các hoạt động điều hành, xử lý công việc trên môi trường mạng. Các loại mã độc hay được sử dụng: *Trojan-Dropper, Trojan-Spy, Trojan-Downloader, Backdoor.win32, ...* Tin tặc thực hiện các chiến dịch tấn công bằng nhiều hình thức khác nhau như thông qua email, tấn công trực tiếp vào các Cổng thông tin điện tử của các bộ ngành, các website cung cấp dịch vụ công và thực hiện chèn mã độc vào các tài liệu, các tập tin cài đặt chương trình đang có sẵn trên các Cổng thông tin điện tử của các bộ ngành và các website cung cấp dịch vụ công. Khi người dùng thực hiện tải về sử dụng, máy tính sẽ nhiễm mã độc, bị kiểm soát và các tài liệu trên máy sẽ bị đánh cắp.

Chữ ký số là giải pháp đảm bảo an toàn thông tin được ứng dụng để đảm bảo tính xác thực, toàn vẹn và chống chối bỏ. Tuy nhiên gần đây các nhà nghiên cứu từ đại học Ruhr Bochum (Đức) đã tiết lộ các phương thức tấn công mới có tên là Shadow Attack lên các tập tin PDF được ký số. Các kỹ thuật tấn công này cho phép tin tặc ẩn và thay thế nội dung trong tài liệu PDF đã ký số mà không làm vô hiệu chữ ký. Tin tặc có thể tạo một tài liệu với hai nội dung khác nhau, một nội dung mà người ký thấy và một nội dung khác mà người nhận tài liệu nhìn thấy. Do đó, mục đích của hướng dẫn này là giúp các cán bộ, công chức, viên chức đã, đang và sẽ sử dụng chữ ký số chuyên dùng Chính phủ bổ sung những kiến thức và công cụ cơ bản để sử dụng chữ ký số một cách an toàn.

1. Các nguy cơ mất an toàn thông tin và nguyên nhân

Các phần mềm độc hại, gián điệp phát tán theo tệp văn bản, ảnh động, đường link đính kèm thông qua thư điện tử, tin nhắn... hoặc tự động lây lan khi người sử dụng cắm USB đã bị nhiễm từ máy tính này sang máy tính khác. Chúng có thể thu thập các thông tin quan trọng rồi tự động gửi về các máy chủ ở nước ngoài.

Máy tính của người dùng có thể bị xâm nhập trái phép thông qua các lỗ hổng bảo mật của hệ điều hành và các ứng dụng nhằm toàn quyền điều khiển, khai thác, lấy cắp và sử dụng thông tin cá nhân cho các mục đích khác.

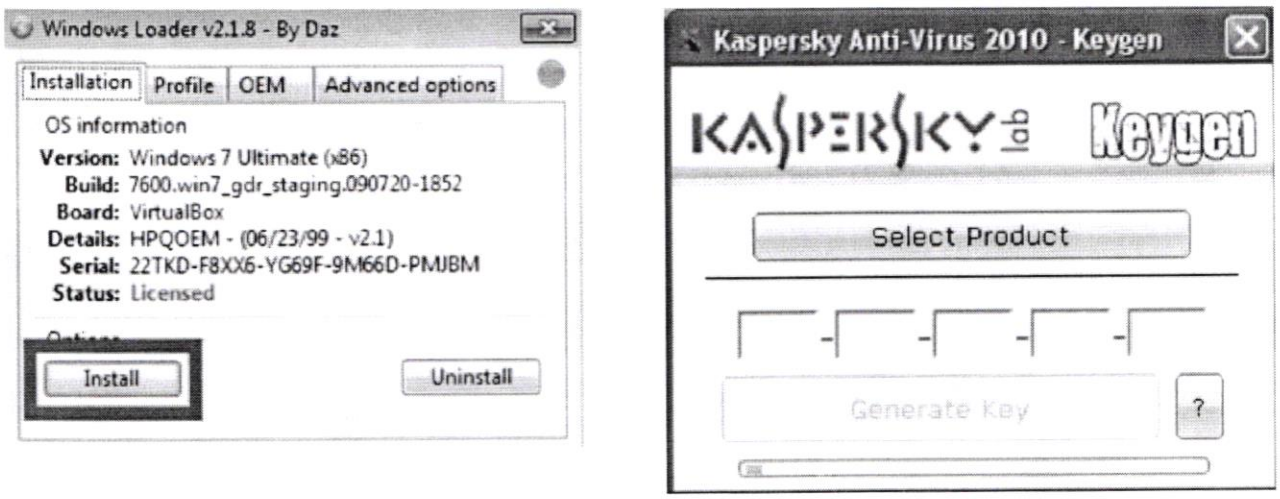
Việc mất mát, thất lạc laptop, thiết bị lưu trữ di động, điện thoại di động... trong đó có chứa các dữ liệu quan trọng.

Các nguyên nhân chủ yếu đó là người sử dụng chưa có hiểu biết hoặc chủ quan, mất cảnh giác với các nguy cơ gây mất an toàn thông tin; chưa thực hiện đúng các quy trình kỹ thuật; máy tính, mạng máy tĩnh chưa được thiết lập các chính sách đảm bảo an toàn thông tin, công tác quản lý, giám sát kỹ thuật còn nhiều sơ hở.

2. Thiết lập máy tính mới an toàn

Các nguy cơ mất an toàn thông tin có thể lập tức ảnh hưởng đến chúng ta ngay sau khi sử dụng máy tính mới mua hoặc mới cài đặt lại. Sau đây là một số lưu ý để thiết lập máy tính mới an toàn chống lại các nguy cơ tấn công:

Với các máy tính mới mua chưa có hệ điều hành cần phải được cài đặt hệ điều hành từ các đĩa cài đặt phần mềm bản quyền hoặc chỉ tải các tập tin cài đặt từ các trang web của nhà sản xuất (cần kiểm tra mã băm khi tải các tập tin cài đặt này) tránh trường hợp tải phải phiên bản "giả mạo" kèm sẵn mã độc, tương tự đối với các ứng dụng phổ biến như ứng dụng văn phòng, bộ gõ tiếng Việt... tuyệt đối không sử dụng các phần mềm bẻ khóa (crack) vì các kẻ tấn công thường gắn mã độc hại trong các phần mềm này để phát tán.



Các phần mềm bẻ khóa, keygen thường chứa mã độc

Khi cài đặt xong nên thiết lập máy tính ở quyền người dùng (User), không nên sử dụng quyền quản trị viên (Administrator). Các máy tính mới thường được nhà sản xuất cài đặt sẵn một số chương trình để quảng cáo, giới thiệu hoặc bản dùng thử của các phần mềm. Các phần mềm này có thể chứa sẵn các nguy cơ mất an toàn thông tin. Do đó người dùng nên gỡ bỏ các chương trình không cần thiết trên máy tính của mình ngay trong quá trình thiết lập ban đầu.

Ngay sau khi cài hệ điều hành cần cài đặt và định kỳ quét toàn bộ máy tính bằng phần mềm diệt vi-rút có bản quyền. Trên thị trường hiện nay có rất nhiều phần mềm diệt vi-rút miễn phí và có trả phí. Cần lưu ý là các chương trình miễn phí có thể ít chức năng hơn nhưng vẫn có thể giúp người dùng cơ bản chống lại các mã độc phổ biến.

Một số phần mềm diệt vi-rút trong và ngoài nước

Cần lưu ý rằng có một số loại mã độc giả mạo chính phần mềm diệt vi-rút. Do đó người dùng cũng cần phải tải tập tin cài đặt chương trình diệt vi-rút từ chính trang web của nhà sản xuất.
Trong quá trình sử dụng, người sử dụng cần định kỳ kiểm tra và cập nhật các bản vá lỗi, lỗ hổng bảo mật cho hệ điều hành và phần mềm ứng dụng. Người sử dụng cũng cần thường xuyên thay đổi mật khẩu và sử dụng mật khẩu mạnh: Mật khẩu độ dài tối thiểu có 8 ký tự gồm ***chữ số, chữ cái*** (thường và hoa) và ***ký tự đặc biệt***. Cần nhớ rằng mật khẩu mạnh sẽ bảo vệ máy tính trong suốt quá trình sử dụng về sau. Mật khẩu mạnh còn giúp bảo vệ cặp khóa trong trường hợp thất lạc thiết bị lưu khóa bí mật, kẻ xấu chiếm được thiết bị token lưu khóa cũng không thể ký mạo danh được.
Thường xuyên sao lưu các dữ liệu quan trọng, dùng CD, DVD, ổ cứng hay trên các phương tiện lưu trữ khác. Cần thận trọng khi sử dụng thiết bị lưu trữ USB khi sao lưu dữ liệu giữa các máy tính. Hiện nay một số hãng cho phép mã hóa các dữ liệu sao lưu trên các thiết bị lưu trữ ngoài để bảo đảm tính bí mật của dữ liệu.

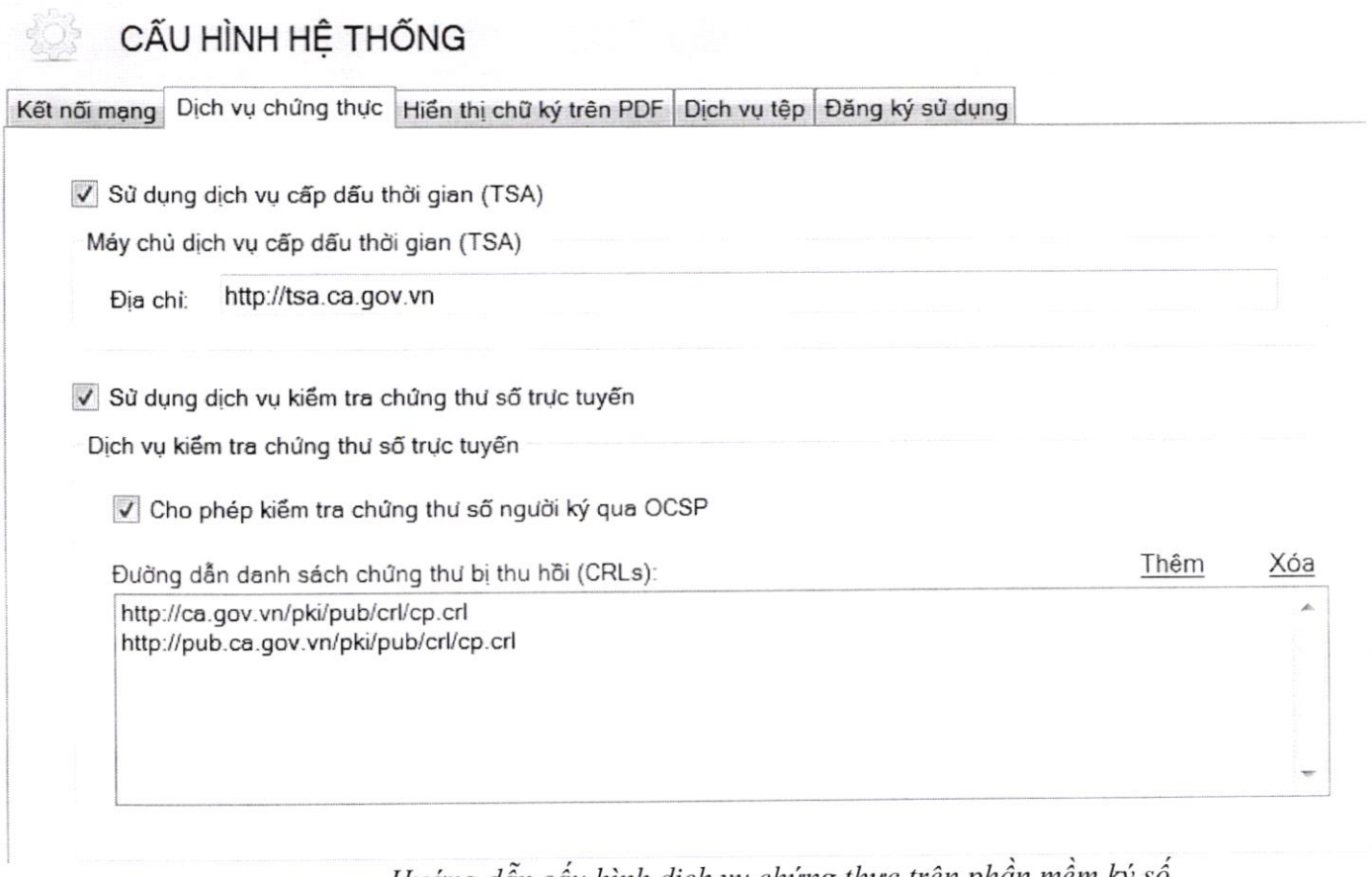
3. Cài đặt, cấu hình các phần mềm ký số an toàn

Để thực hiện ký số, đầu tiên cần cài đặt phần mềm điều khiển thiết bị (driver) token ký số. Người sử dụng chữ ký số chuyên dùng Chính phủ truy cập trang web để tải các phần mềm driver và ký số như VsignPDF, bộ công cụ tích hợp ký số theo Nghị định 30/2020/NĐ-CP ngày 05/03/2020 của Chính phủ về công tác văn thư tại địa chỉ sau:
https://dvc.ca.gov.vn/tai-phan-mem
Một chính sách bắt buộc đối với người sử dụng máy tính là khi tải bất cứ phần mềm nào trên mạng về trước khi cài đặt chúng ta đều nên quét mã độc trước khi thực hiện cài đặt. Công cụ quét mã độc được Ban Cơ yếu Chính phủ cung cấp tại địa chỉ sau:
http://av.bcy.gov.vn
Căn cứ Điều 9 của Nghị định 130/2018/NĐ-CP ngày 27/9/2018 của Chính phủ quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số, điều kiện đảm bảo an toàn cho chữ ký số cụ thể như sau:
- Chữ ký số được tạo ra trong thời gian chứng thư số có hiệu lực và kiểm tra được bằng khóa công khai ghi trên chứng thư số đó.
- Chữ ký số được tạo ra bằng việc sử dụng khóa bí mật tương ứng với khóa công khai ghi trên chứng thư số do một trong các tổ chức được pháp luật quy định cấp.
- Khóa bí mật chỉ thuộc sự kiểm soát của người ký tại thời điểm ký.

Vì vậy, trong quá trình thực hiện ký số, xác thực cần lưu ý đến hai dịch vụ của Ban Cơ yếu Chính phủ cung cấp để đảm bảo an toàn cho chữ ký số, cụ thể:
(1) Kiểm tra chứng thư số trực tuyến: Tác vụ này sẽ kết nối tới máy chủ của Ban Cơ yếu Chính phủ và kiểm tra xem chứng thư số còn hiệu lực hay không trước khi tiến hành ký số. Việc kiểm tra chữ ký số này có thể thực hiện thông qua 02 hình thức đó là kiểm tra danh sách hủy bỏ (CRLs) hoặc kiểm tra trạng thái chứng thư số trực tuyến (OCSP).
Thư viện sẽ tự động kiểm tra chứng thư số cần kiểm tra và trả về kết quả. Nội dung chứng thư số cần kiểm tra để đảm bảo tính xác thực, toàn vẹn:
- Chứng thư số có phải do Ban Cơ yếu Chính phủ cung cấp hay không;
- Kiểm tra thời gian hợp lệ của chứng thư số;
- Kiểm tra chứng thư số đã bị hủy bỏ hay chưa.

(2) Lấy dấu thời gian: Để xác định thời gian ký số, trong quá trình ký số các thư viện sẽ kết nối tới máy chủ cấp dấu thời gian của Ban Cơ yếu Chính phủ. Đồng thời, cho phép xác định chính xác thời điểm người sử dụng ký số.
(Lưu ý: thời gian lấy từ máy chủ, không phải thời gian máy tính cá nhân của người sử dụng).
Sau đây là địa chỉ truy cập các dịch vụ trực tuyến:
- Danh sách hủy bỏ (CRLs): *http://ca.gov.vn/pki/pub/crl/cp.crl*
- Kiểm tra tình trạng chứng thư số trực tuyến (OCSP): *http://ocsp.ca.gov.vn*
- Máy chủ dấu thời gian: *http://tsa.ca.gov.vn*

Thông tin chi tiết tài liệu, phần mềm, mã nguồn tại địa chỉ: *http://ca.gov.vn*
Ngoài ra người sử dụng có thể tham khảo các video hướng dẫn cài đặt, cấu hình các phần mềm ký số tại địa chỉ sau: *https://dvc.ca.gov.vn/video-huong-dan-cai-dat-su-dung*



Hướng dẫn cấu hình dịch vụ chứng thực trên phần mềm ký số

4. Bảo quản, sử dụng thiết bị lưu khóa bí mật an toàn

Thiết bị lưu khóa bí mật của người sử dụng chữ ký số chuyên dùng Chính phủ là thiết bị PKI Token được Ban Cơ yếu cấp có chứa cặp khóa bí mật/công khai và Chứng thư số cấp cho người sử dụng. Việc thực hiện ký số không thể thiếu thiết bị Token và mật khẩu.

Tổ chức quản lý cần ban hành quy chế quản lý, sử dụng thiết bị PKI Token dành cho người sử dụng. Các cá nhân có trách nhiệm bảo quản token an toàn và đặt mật khẩu mạnh để bảo vệ an toàn cho cặp khóa của mình.

Người sử dụng có thể áp dụng quy tắc đặt mật khẩu mạnh mà vẫn dễ nhớ đó là thay đổi các chữ cái tạo nên mật khẩu từ những thông tin gắn với bản thân, hoặc kết hợp các chữ cái có trong các từ của một câu nói yêu thích, ví dụ về những mật khẩu mạnh là: ***88V1nhpHuc{cke-peak}amp;, $H@idUong34%, #T3x1LtyVn$#***

Để đánh giá độ mạnh và kiểm tra mật khẩu sử dụng có nằm trong các bộ từ điển hoặc cơ sở dữ liệu mật khẩu đã bị bẻ khóa không chúng ta có thể kiểm tra thông qua các địa chỉ sau:

https://password.kaspersky.com/

Không giao Token của mình cho người khác sử dụng và tuyệt đối không cho người khác biết mật khẩu Token của mình.

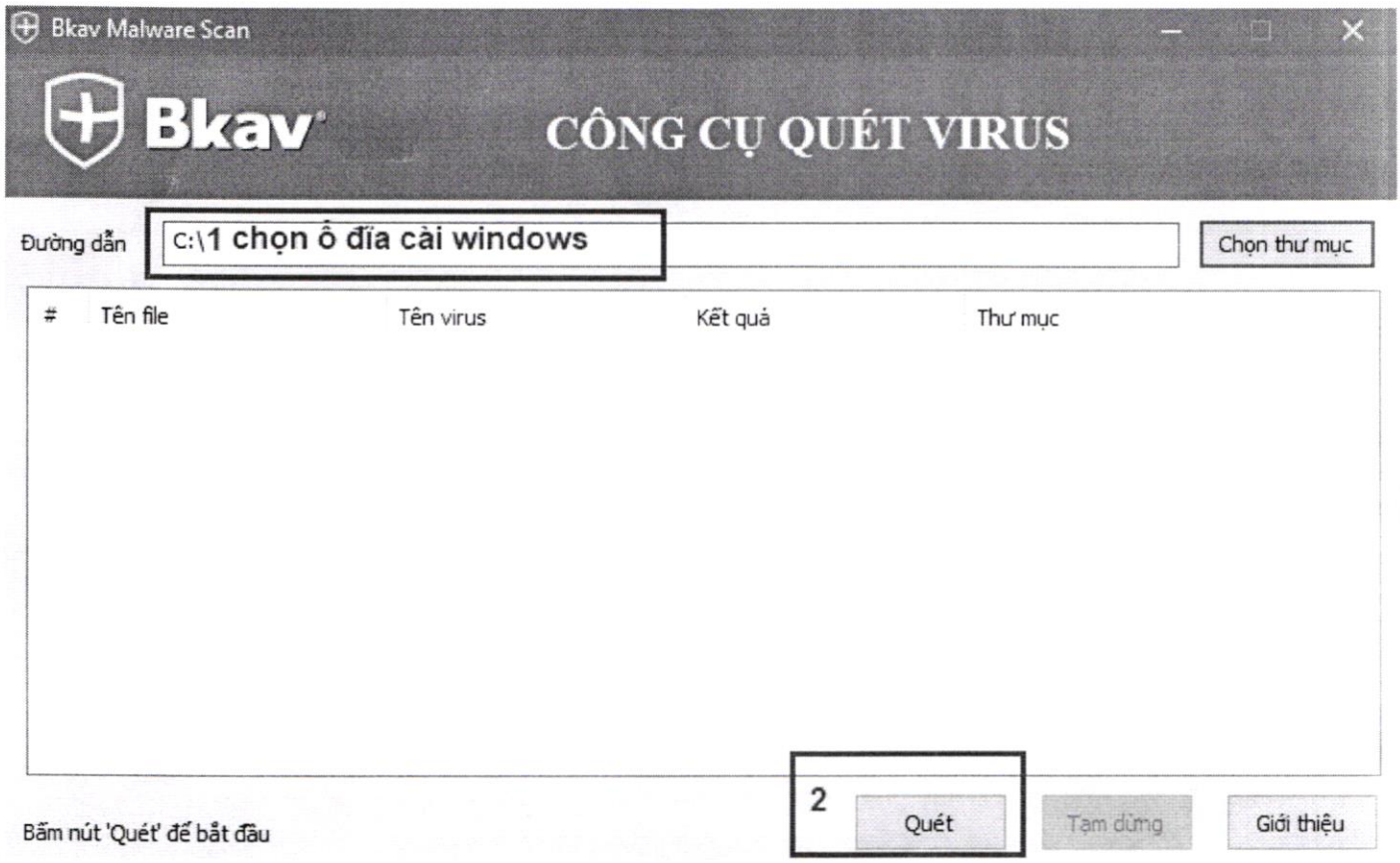
5. Hướng dẫn nhanh rà quét mã độc trên máy tính người dùng

Để thực hiện nhanh rà quét, gỡ bỏ mã độc, người dùng cần thực hiện các bước cụ thể, như sau:

Bước 1: Tải công cụ rà quét mã độc tại địa chỉ:

http://ca.gov.vn/MalwareRemoverTool.rar

Bước 2: Giải nén và chạy công cụ, thực hiện như hình dưới để rà quét nhanh.

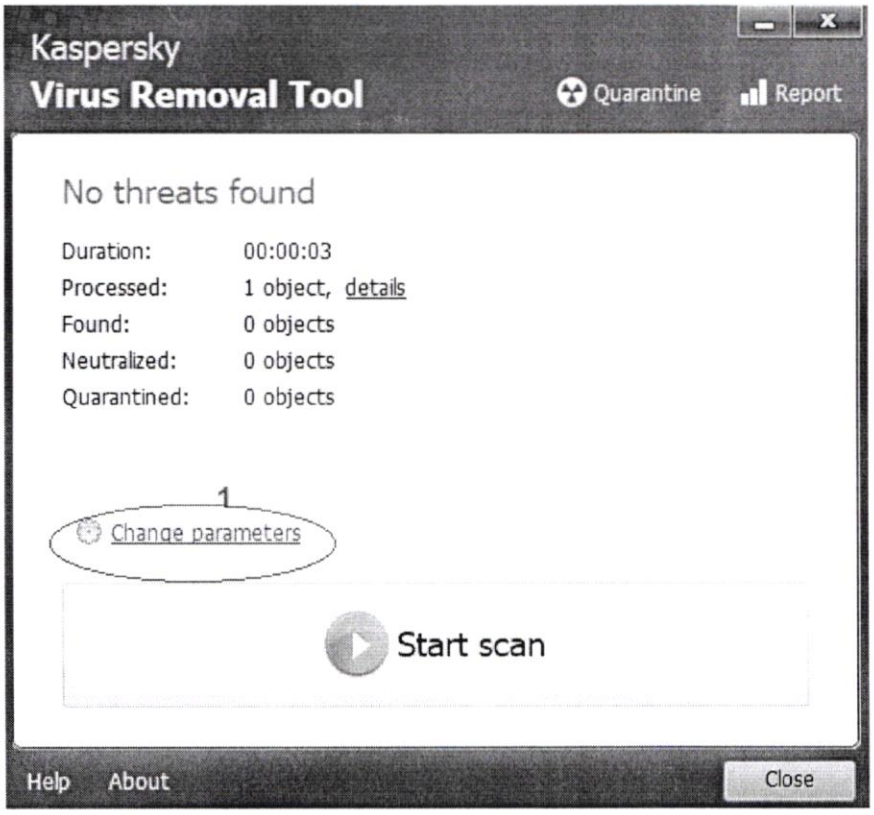


Bước 3: Trường hợp công cụ rà quét phát hiện ra mã độc và diệt thì người dùng thực hiện tải công cụ dưới đây để rà quét toàn bộ máy tính.

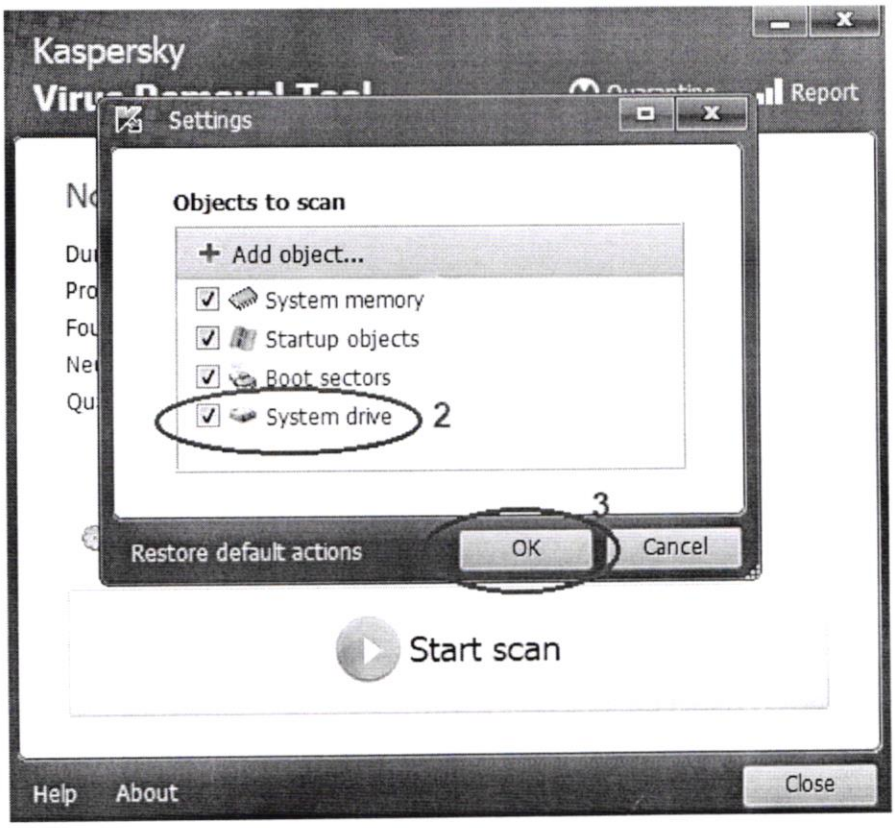
http://av.bcy.gov.vn/Malware%20Remove%20Tool.exe

Thực hiện theo hình ảnh hướng dẫn dưới đây:

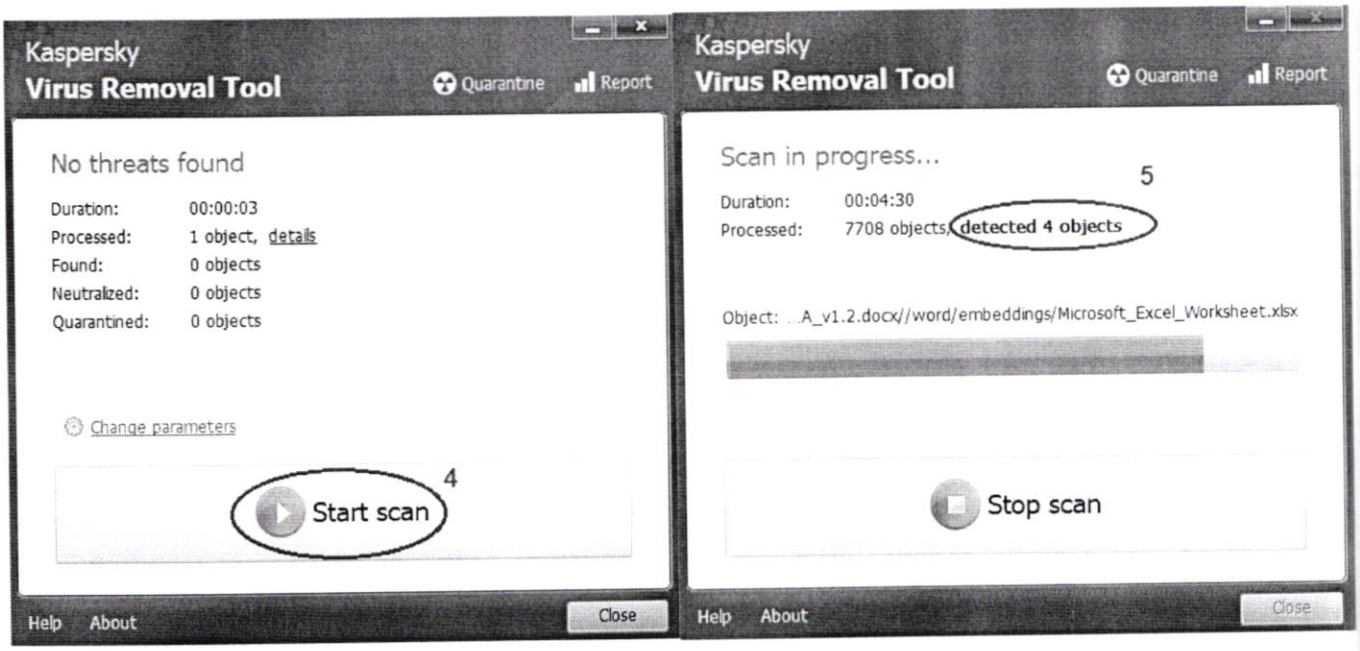
- Chọn các các đối tượng để rà quét.



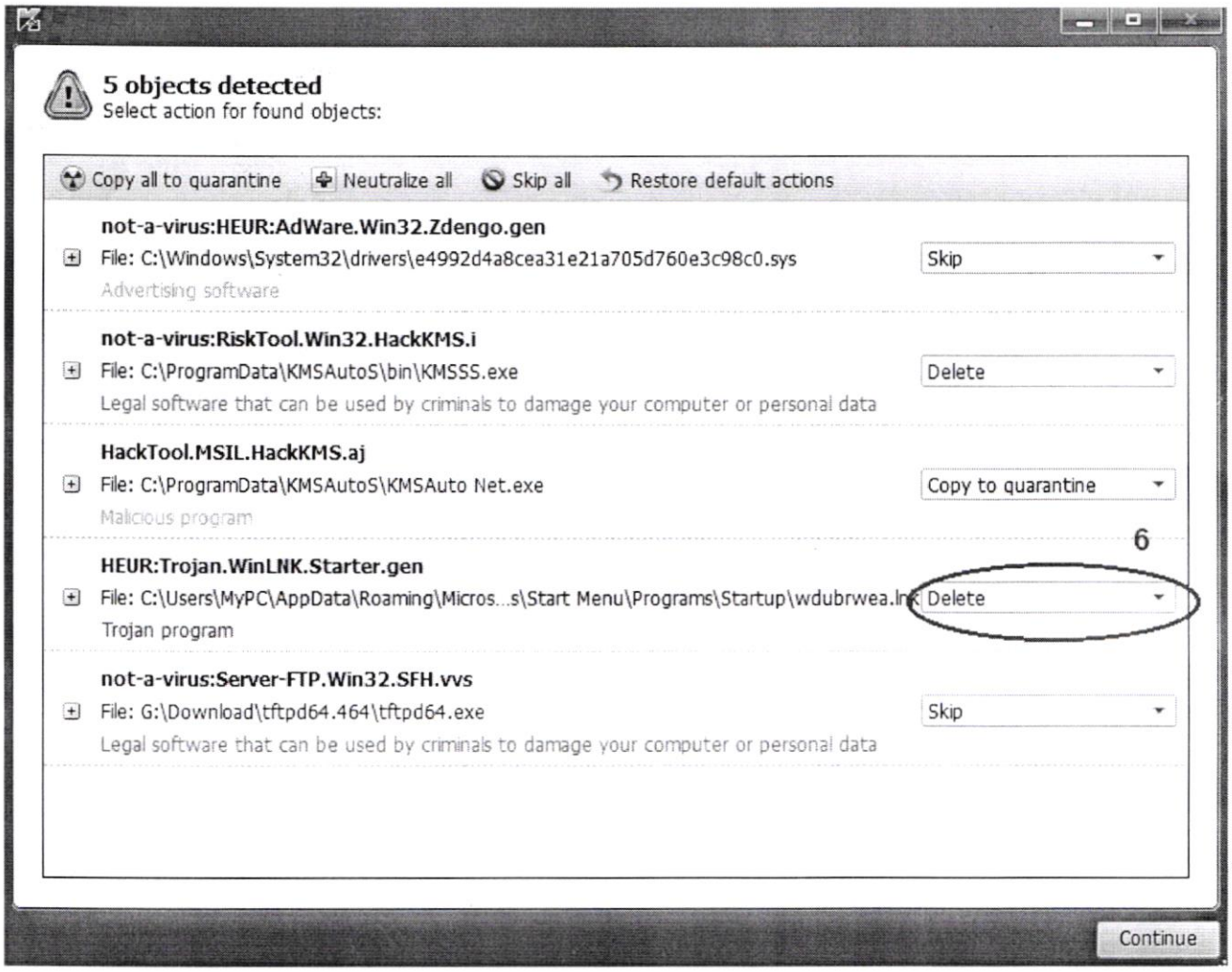
- Chọn các ổ đĩa của máy tính và Nhấn **OK** để tiếp tục.



- Nhấn **Start scan** để bắt quét virus



Trường hợp công cụ có phát hiện virus trên máy tính, người dùng nên lựa chọn thao tác xóa bỏ như hình dưới đây.



Trong quá trình thực hiện, nếu có vướng mắc, đề nghị liên hệ với Cục Chứng thực số và Bảo mật thông tin qua địa chỉ email: ca@bcy.gov.vn hoặc số điện thoại: **0243 773 8668** để được hỗ trợ, giải quyết.

BAN CƠ YẾU CHÍNH PHỦ
CỤC CHỨNG THỰC SỐ VÀ BẢO MẬT THÔNG TIN

Số: 458 /CTSBMTT-QTHT
V/v đảm bảo an toàn thông tin trong sử dụng dịch vụ chữ ký số chuyên dùng Chính phủ

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 16 tháng 12 năm 2020

Kính gửi:
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Cơ quan chuyên trách về Công nghệ thông tin các Bộ, Ngành.

Trong thời gian gần đây, thông qua hệ thống theo dõi giám sát và phân tích mã độc của Trung tâm Công nghệ thông tin và Giám sát an ninh mạng - Ban Cơ yếu Chính phủ đã phát hiện nhiều chiến dịch tấn công có chủ đích sử dụng mã độc vào máy tính người dùng tại các cơ quan Đảng và Nhà nước. Ngày 02/10/2020 Trung tâm Công nghệ thông tin và Giám sát an ninh mạng đã có văn bản số 398/CNTTGSM-ANM gửi các cơ quan, đơn vị về việc rà soát mã độc và khuyến cáo các nguy cơ tấn công mạng. Để tăng cường việc đảm bảo an toàn thông tin cho các hoạt động ứng dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ, Cục Chứng thực số và Bảo mật thông tin đề nghị các cơ quan, đơn vị một số nội dung như sau:

1. Thường xuyên thực hiện đánh giá, rà quét mã độc các máy tính của cơ quan, đơn vị. Triển khai cài đặt phần mềm quét virus có bản quyền, công cụ để kiểm tra, rà quét mã độc có thể tải tại địa chỉ: http://av.bcy.gov.vn.

2. Khuyến cáo các đơn vị thuộc phạm vi quản lý và các đơn vị liên quan cảnh báo, nâng cao nhận thức về an toàn an ninh mạng nói chung và cảnh giác với nguy cơ tấn công mạng có chủ đích nói riêng.

3. Thực hiện theo hướng dẫn đảm bảo an toàn thông tin trong sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ tại địa chỉ https://ca.gov.vn/.

Trong quá trình triển khai thực hiện, nếu có vướng mắc đề nghị các cơ quan, đơn vị liên hệ với Cục Chứng thực số và Bảo mật thông tin qua địa chỉ email: ca@bcy.gov.vn hoặc số điện thoại: 0243.7738668 để phối hợp, giải quyết.

Trân trọng./.

Nơi nhận:
- Như trên;
- Đ/c PTB Nguyễn Đăng Lực (để b/c);
- Lưu: VT, QTHT. DS95b.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC CHỨNG THỰC SỐ VÀ BẢO MẬT THÔNG TIN
BAN CƠ YẾU CHÍNH PHỦ

Lê Quang Tùng