ỦY BAN NHÂN DÂN **HUYỆN TÂY SƠN**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1081 /UBND-CNTT V/v thực hiện kiểm tra, rà soát lỗ hổng đối với Cổng thông tin điện tử và thiết bị được dùng để ký số	*Tây Sơn, ngày28 tháng 12 năm 2020*

Kính gửi:

- Các phòng, ban, ngành huyện;
- UBND các xã, thị trấn.

Theo báo cáo tình hình an toàn thông tin của Cục An toàn thông tin và kết quả theo dõi, giám sát của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đã ghi nhận và phát hiện nhiều chiến dịch tấn công có chủ đích sử dụng mã độc vào máy tính người dùng, trong đó có các máy tính sử dụng chữ ký số chuyên dùng Chính phủ và các Cổng/Trang thông tin điện tử (website) của các cơ quan nhà nước (*.binhdinh.gov.vn). Sự việc này có thể trở nên rất nguy hiểm và nhạy cảm nếu đối tượng chống phá lợi dụng để đăng tải, phát tán những nội dung xấu, độc, xuyên tạc về chủ quyền, chủ trương chính sách của Đảng và Nhà nước,... đặc biệt trong giai đoạn chuẩn bị trước thềm Đại hội Đảng toàn quốc lần thứ XIII.

Theo đề nghị của Sở Thông tin và Truyền thông tỉnh Bình Định tại Văn bản số 1256/STTTT-BCVT&CNTT ngày 22 tháng 12 năm 2020 về việc thực hiện kiểm tra, rà soát lỗ hổng đối với trang thông tin điện tử và thiết bị được dùng ký số; Chủ tịch UBND huyện có ý kiến như sau:

1. Giao Văn phòng HĐND và UBND huyện rà soát, xác minh và xử lý việc tấn công có chủ đích sử dụng mã độc đối với Cổng thông tin điện tử UBND huyện.

(Tham khảo hướng dẫn tại Phụ lục 01 kèm theo)

2. Đề nghị các phòng, ban, ngành huyện, UBND các xã, thị trấn thực hiện một số nhiệm vụ sau:

- Đảm bảo an toàn thông tin trong sử dụng chữ ký số chuyên dùng Chính phủ.

- Thông báo, tuyên truyền nội dung hướng dẫn đảm bảo an toàn thông tin cho tất cả cán bộ, công chức, viên chức, người lao động sử dụng chữ ký số chuyên dùng của Chính phủ trong cơ quan, đơn vị, địa phương mình để biết, thực hiện.

(Tham khảo hướng dẫn tại Phụ lục 02 kèm theo)

Trong quá trình triển khai nếu cần hỗ trợ liên hệ: Phòng Bưu chính, Viễn thông và Công nghệ thông tin - Sở Thông tin và Truyền thông tỉnh Bình Định, điện thoại: 02562.210517; Trung tâm Công nghệ thông tin và Truyền thông tỉnh Bình Định, điện thoại: 0256.3811626; Văn phòng HĐND và UBND huyện, điện thoại: 02563.880761 để được hướng dẫn, giải đáp.

Đề nghị các phòng, ban, ngành huyện, UBND các xã, thị trấn triển khai thực hiện./.

Nơi nhận:
- Như trên;
- CT, PCT UBND huyện;
- Lãnh đạo VP;
- Lưu: VT.

KT.CHỦ TỊCH
PHÓ CHỦ TỊCH

Bùi Văn Mỹ

Phụ lục 01

HƯỚNG DẪN KIỂM TRA, RÀ SOÁT CỔNG THÔNG TIN ĐIỆN TỬ

Theo kết quả rà soát, phân tích của Trung tâm NCSC thì đây không phải dấu hiệu tấn công mạng vào hàng loạt các hệ thống website, tuy nhiên, một số đối tượng xấu đã lợi dụng những tính năng cho phép người dùng bình thường tương tác, gửi thông tin lên website như tính năng của các chuyên mục "Hỏi đáp, Lấy ý kiến, Diễn đàn, Phản hồi,..." nhằm gắn các đường dẫn (backlink) quảng cáo để tăng tuy tín, có thêm lượng truy cập từ các công cụ tìm kiếm. Phần lớn nguyên nhân của hiện tượng này là do các website không sử dụng tính năng kiểm duyệt nội dung người dùng đưa lên trước khi công khai. Để đảm bảo an toàn thông tin cho website mà đơn vị đang quản lý, đề nghị:

1. Liệt kê, kiểm tra nhanh toàn bộ website, hệ thống mà đơn vị đang quản lý để chủ động kiểm tra, rà soát tình trạng lạm dụng

- Thực hiện rà soát toàn bộ domain, subdomain đang quản lý để chủ động rà quét, tránh bỏ sót. Rà soát lại các hệ thống không còn sử dụng và cân nhắc tạm thời ngắt kết nối/vô hiệu hoá nếu không sử dụng.

- Có thể kết hợp việc thông kê thông tin nội bộ với sử dụng công cụ hỗ trợ kiểm tra online: https://hackertarget.com/find-dns-host-records

2. Rà soát kết quả trên công cụ tìm kiếm Google

Tìm kiếm nhanh các bài viết có dấu hiệu bị chèn backlink trên Google sử dụng cấu trúc tìm kiếm: "[từ khóa lạm dụng]" site:[donvi.gov.vn].

Ví dụ: Kết quả của câu tìm kiếm "truyện sex" trên các website abc.gov.vn

"truyện sex" site:abc.gov.vn

Lưu ý: Nội dung từ khóa có thể mở rộng thêm tùy vào đặc thù của đơn vị chủ quản.

3. Rà soát trong hệ thống quản trị nội dung, cơ sở dữ liệu

Quản trị viên website cần thực hiện một số công việc sau, đặc biệt lưu ý các chức năng cho phép người dùng có thể tự đăng nội dung lên như Bình luận, Hỏi đáp:

- Kiểm tra rà soát các từ khóa bằng công cụ tìm kiếm của website.

- Rà soát các nội dung bài viết, bình luận đã đăng tải. Rà soát thêm trên cơ sở dữ liệu nếu cần thiết.

- Cấu hình siết chặt việc kiểm duyệt nội dung trước khi đăng lên website của đơn vị.

Phụ lục 02
HƯỚNG DẪN ĐẢM BẢO AN TOÀN THÔNG TIN CHO NGƯỜI SỬ DỤNG CHỮ KÝ SỐ CHUYÊN DÙNG CỦA CHÍNH PHỦ

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.

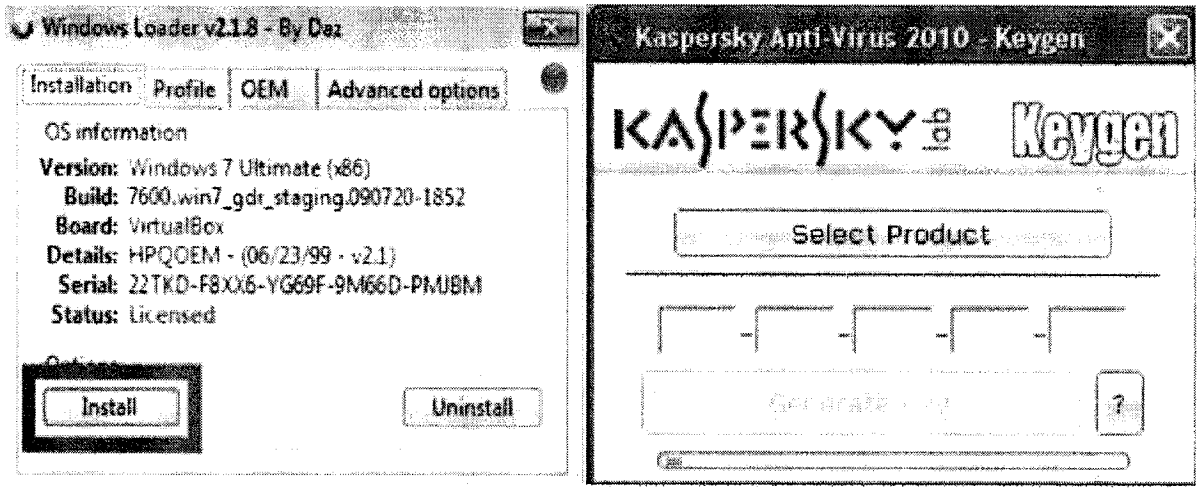
Việc mất mát, thất lạc laptop, thiết bị lưu trữ di động, điện thoại di động... trong đó có chứa các dữ liệu quan trọng.

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. 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

Một số phần mềm diệt vi-rút trong và ngoài

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:

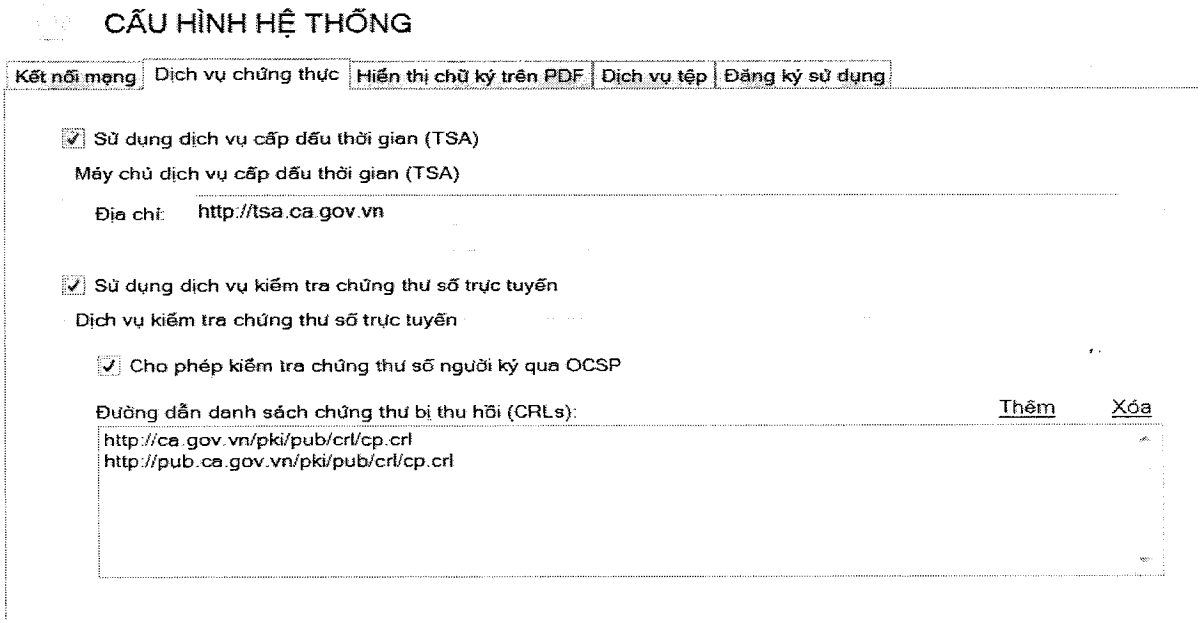
- Danh sách hủy bỏ (CRLs): *http://ca.gov.vn/pki/pub/crl/cp.crl*

- 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

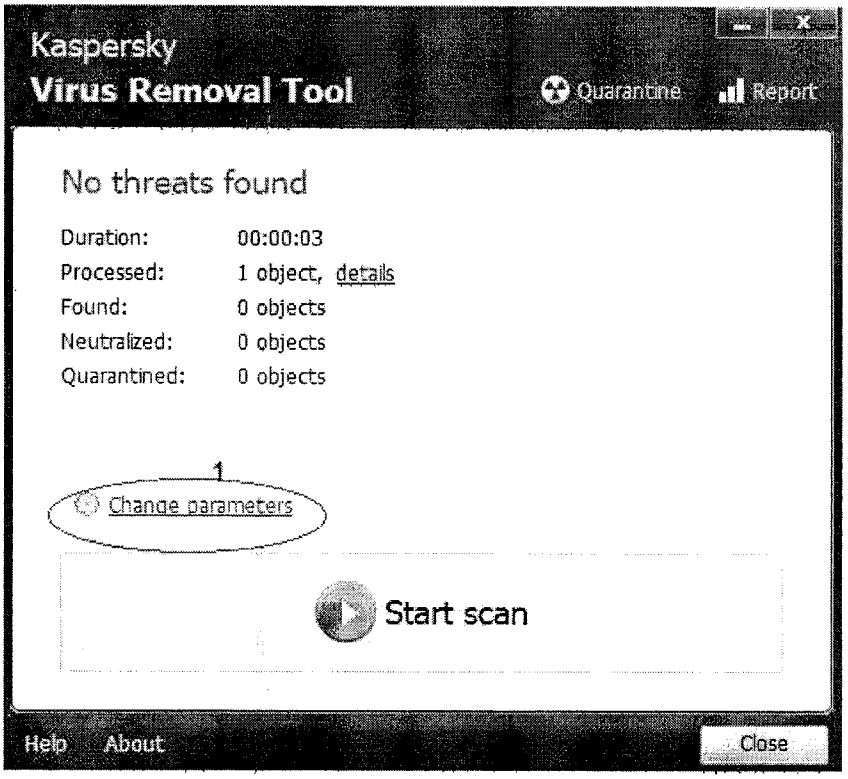
Để thực hiện nhanh rà quét, gỡ bỏ mã độc, người dùng cần thực hiện các bước cụ thể, như sau:

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

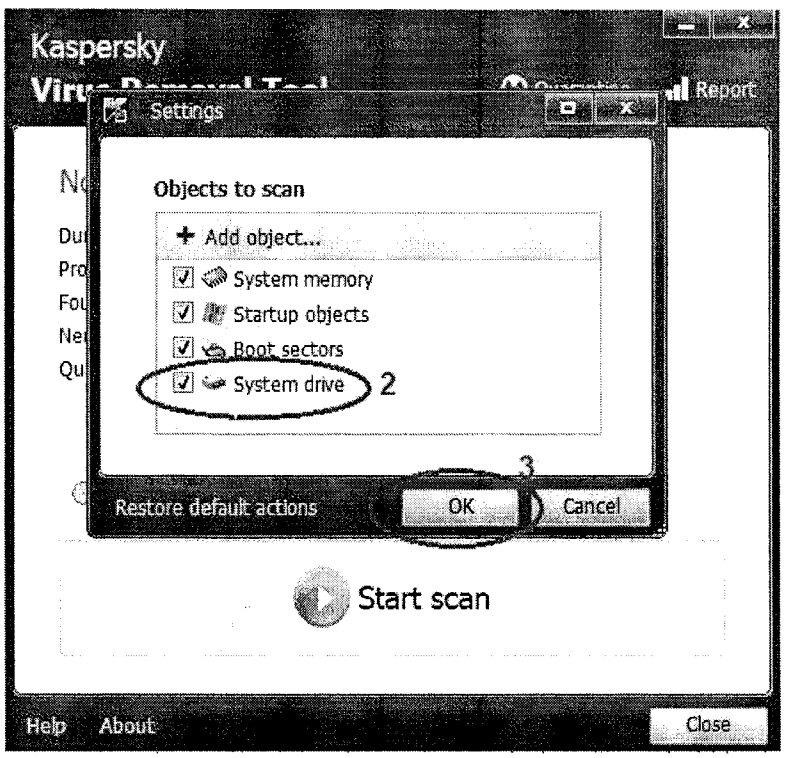
http://av.bcy.gov.vn/Malware%20Remove%20Tool.exe

Bước 2: Mở công cụ vừa tải và thực theo hình ảnh dưới đây:

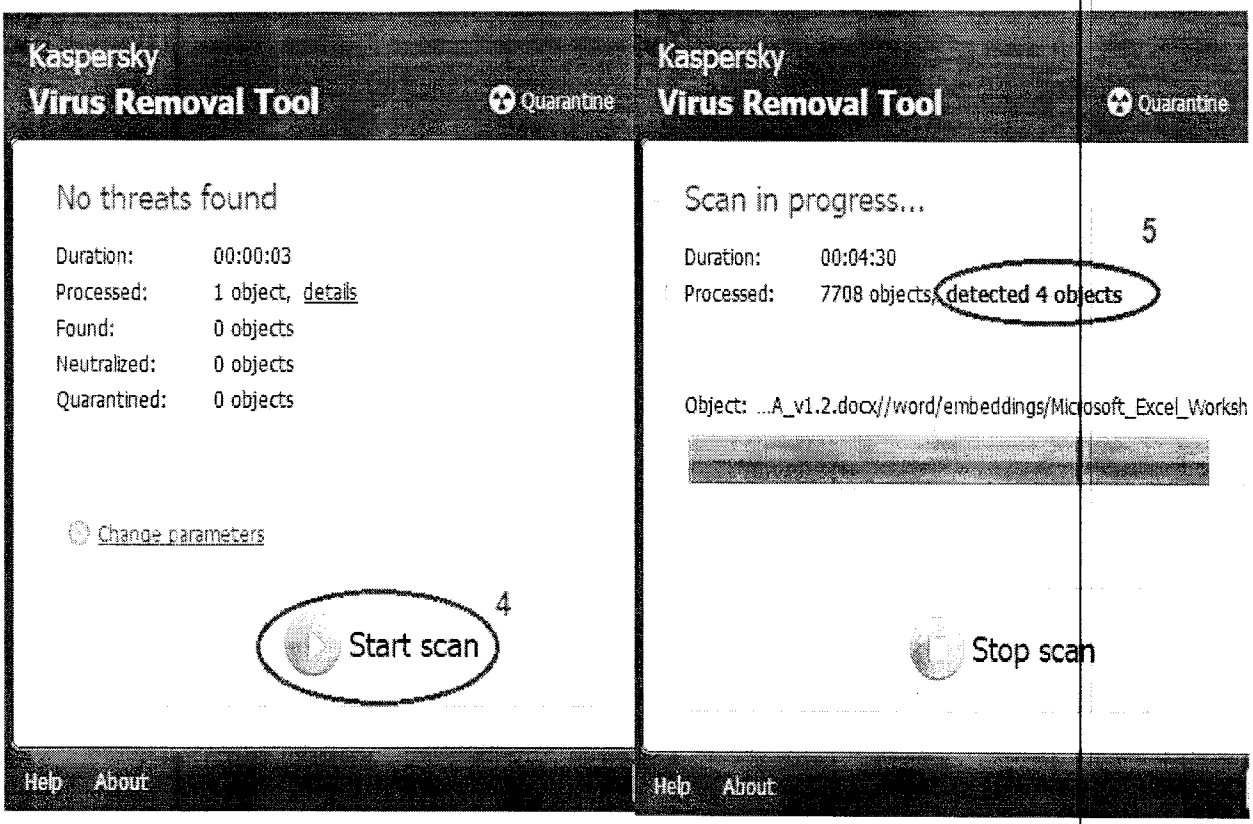
- Chọn các các đối tượng để rà quét.



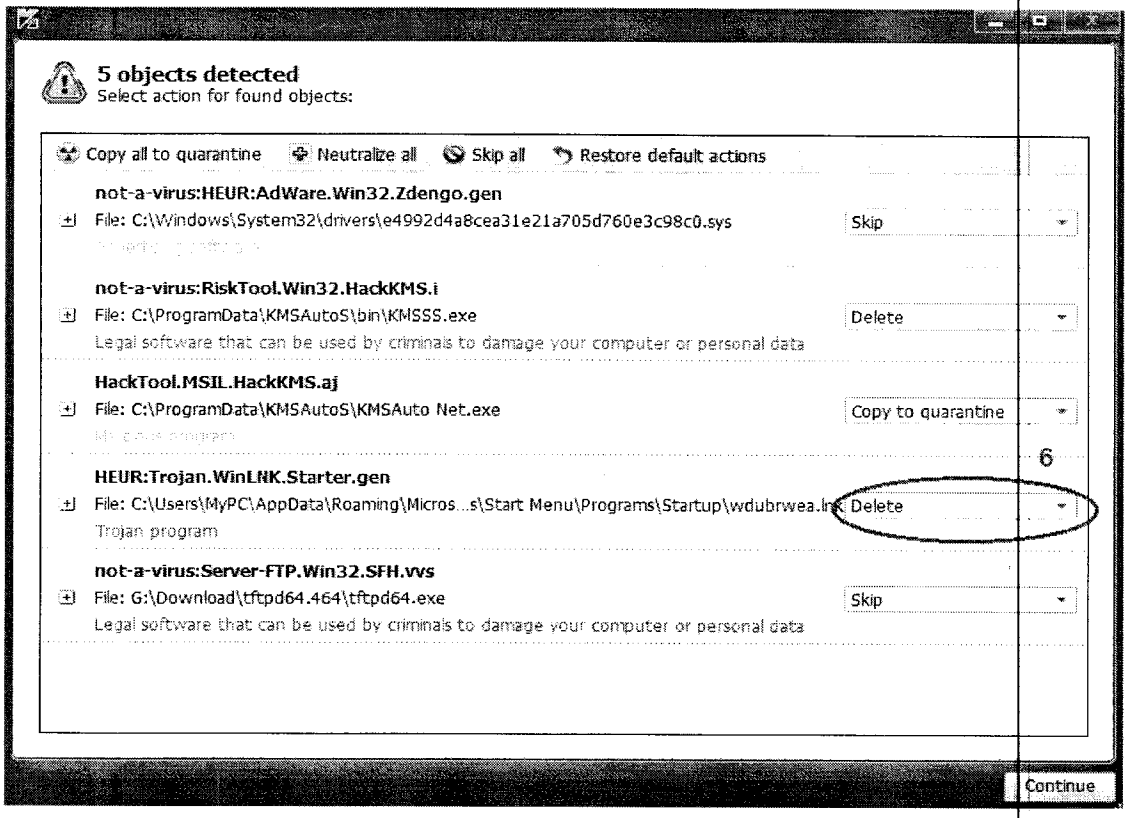
- Chọn các ổ đĩa của máy tính và Nhấn **OK** để tiếp tục.



- 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.



Tham khảo

1. http://antoanthongtin.gov.vn
2. https://dvc.ca.gov.vn