(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0051147**

(51)[7] **G06F 21/00**

(13) **B**

(21) 1-2012-00904

(22) 03/04/2012

(45) 25/09/2025 450

(43) 25/12/2012 297A

(73) Công ty cổ phần BKAV (VN)
Tầng 2, toà nhà HH1-khu đô thị Yên Hoà, phường Yên Hoà, quận Cầu Giấy, thành phố Hà Nội

(72) Vũ Ngọc Sơn (VN); Nguyễn Tử Quảng (VN).

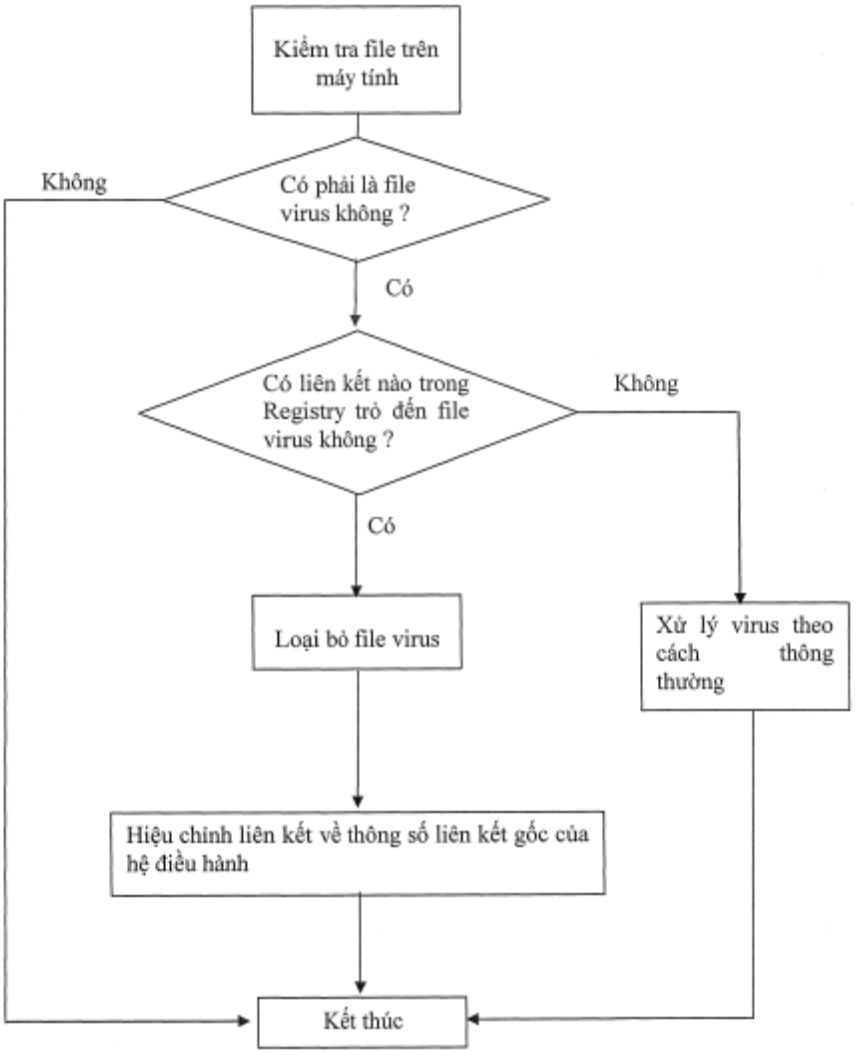
(74) Công ty TNHH Tư vấn đầu tư và Sở hữu trí tuệ Hoàng Phi (HOANG PHI INVEST & I.P CO., LTD)

(54) PHƯƠNG PHÁP DIỆT VIRUS MÁY VI TÍNH LOẠI LÂY SÂU VÀO HỆ THỐNG KHÔNG LÀM ẢNH HƯỞNG ĐẾN HOẠT ĐỘNG BÌNH THƯỜNG CỦA HỆ ĐIỀU HÀNH

(21) 1-2012-00904

(57) Sáng chế đề cập đến phương pháp diệt virus máy vi tính loại lây sâu vào hệ thống không làm ảnh hưởng đến hoạt động bình thường của hệ điều hành, trong đó khắc phục được nhược điểm của các phương pháp diệt virus máy vi tính hiện có trên thị trường bằng cách khôi phục các thông số liên kết gốc trong cơ sở dữ liệu của Registry gốc của hệ thống nhằm đảm bảo việc loại bỏ virus loại lây sâu vào hệ thống mà không làm ảnh hưởng đến sự hoạt động bình thường của hệ điều hành cũng như các phần mềm tiện ích.

HÌNH 4



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp diệt virus, cụ thể là đề cập phương pháp diệt virus loại lây sâu vào hệ thống trên nền máy vi tính sử dụng hệ điều hành như hệ điều hành Microsoft Windows và các hệ điều hành khác cho máy vi tính.

Tình trạng kỹ thuật của sáng chế

Hiện nay, việc sử dụng máy vi tính cài đặt các hệ điều hành như Microsoft Windows, MAC OS, Linux đã trở nên rất phổ biến. Máy vi tính được dùng cho nhiều mục đích khác nhau như làm việc, học tập hoặc giải trí. Để đạt được các mục đích này, mỗi máy vi tính cài đặt một hoặc nhiều phần mềm tiện ích tùy theo mục đích sử dụng cụ thể. Sự hoạt động đúng đắn của hệ điều hành, các phần mềm tiện ích cũng như các thông tin, dữ liệu được lưu trữ trên máy vi tính luôn có nguy cơ bị thay đổi, xóa, sửa hay lấy cắp bởi sự xuất hiện, lây nhiễm, phá hoại của virus máy vi tính. Virus lây nhiễm vào hệ điều hành và các chương trình phần mềm trên nền máy vi tính qua nhiều cách khác nhau như qua các thiết bị lưu trữ di động, ví dụ, đĩa CD, ổ USB, qua thư điện tử (*email*) hoặc qua mạng *internet*. Khi mà nhu cầu sử dụng các thiết bị lưu trữ, nhu cầu giao dịch qua email, *internet* ngày càng cao thì khả năng lây lan virus trên máy vi tính là rất lớn.

Để giúp người sử dụng đối phó với virus, đã có nhiều chương trình phần mềm diệt virus được đưa ra. Các chương trình phần mềm này có chức năng nhận diện các file bị nhiễm virus, sau đó loại bỏ file virus ra khỏi hệ thống, cũng như loại bỏ các thông số liên kết trỏ đến file virus ra khỏi Registry.

Tuy nhiên, trên thực tế đã xuất hiện nhiều loại virus có khả năng chống lại việc loại bỏ chúng ra khỏi hệ thống, cụ thể là virus loại lây sâu vào hệ thống, bằng cách chúng đăng ký và cài đặt lại các thông số liên kết trên hệ thống, để thông số này thay vì trỏ đến file của hệ thống thì trỏ đến file virus, khiến cho khi các phần mềm diệt virus loại bỏ file virus và/hoặc loại bỏ thông số liên kết trỏ đến file virus sẽ làm cho hệ điều hành hoặc phần mềm tiện ích không còn hoạt động được bình thường như trước khi diệt virus.

Để tránh các sửa đổi thông số liên kết gốc trong Registry khiến cho hệ điều hành có thể hoạt động không ổn định, các nhà sản xuất hệ điều hành khuyến cáo có thể thường xuyên sao lưu lại Registry, từ đó khôi phục lại Registry khi hệ điều hành có lỗi. Tuy nhiên, đây không phải là giải pháp có thể áp dụng để diệt virus, thực tế các phần mềm tiện ích hoạt động trên hệ thống cũng sẽ liên tục sửa đổi các thông số liên kết trong Registry để phục vụ hoạt động của phần mềm, việc sao lưu Registry trở nên không khả thi vì sẽ phải sao lưu liên tục, khi hệ điều hành bị lỗi cũng sẽ không biết cần phải khôi phục lại thông số liên kết nào, tại thời điểm nào. Ngoài ra, để sao chép được Registry không có lỗi, phần mềm diệt virus cần phải được cài đặt trên máy vi tính trước khi máy vi tính bị lây nhiễm virus, điều này không phải lúc nào cũng được đảm bảo. Trong trường hợp máy vi tính bị nhiễm virus trước khi cài đặt phần mềm diệt virus, phần mềm diệt virus sẽ không có cơ hội sao lưu được thông số liên kết cũ, dẫn tới không có thông số liên kết cũ để khôi phục lại khi diệt virus.

Như vậy, cần phải có một phương pháp giúp loại bỏ những virus loại lây sâu vào hệ thống như nêu trên ra khỏi hệ thống, đồng thời đảm bảo hệ điều hành và các chương trình phần mềm tiện ích được cài đặt trong máy vi tính vẫn có thể hoạt động bình thường sau khi đã loại bỏ virus.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất phương pháp diệt virus loại lây sâu vào hệ thống, cụ thể là thâm nhập cả vào Registry, trên nền máy vi tính, trong đó khắc phục được nhược điểm của các chương trình phần mềm diệt virus hiện nay, bằng cách đồng

thời loại bỏ file virus và khôi phục lại các thông số liên kết mà virus đã sửa trong Registry khi lây nhiễm vào máy vi tính về thông số liên kết gốc, nhằm đảm bảo việc loại bỏ virus không làm ảnh hưởng đến sự hoạt động bình thường của hệ điều hành cũng như các phần mềm tiện ích. Phương pháp diệt virus theo sáng chế bao gồm các bước:

(i) kiểm tra xem file có phải file virus hay không, bằng đoạn chương trình trong phần mềm hoặc một phần mềm có sẵn chức năng nhận dạng virus theo cách thông thường;

(ii) nếu là file virus, kiểm tra trong Registry hiện tại xem có liên kết nào trỏ tới file virus này không; nếu không có liên kết nào trỏ tới file virus này thì kết thúc việc diệt virus;

(iii) nếu có liên kết trong Registry hiện tại trỏ tới file virus thì

- loại bỏ file virus;
- hiệu chỉnh lại liên kết đang trỏ tới file virus, bằng cách khôi phục lại liên kết gốc từ cơ sở dữ liệu Registry gốc và ghi đè liên kết gốc lên liên kết bị sửa đổi, nhờ đó liên kết bị virus sửa đổi này không trỏ đến file virus nữa và chuyển sang trỏ tới file gốc của hệ điều hành;

Mô tả vắn tắt hình vẽ

Hình 1 thể hiện sơ đồ khối hoạt động bình thường của hệ thống máy tính thông thường khi không bị virus;

Hình 2 thể hiện sơ đồ khối hoạt động của hệ thống khi có sự thâm nhập của file virus loại lây sâu vào hệ thống;

Hình 3 thể hiện sơ đồ khối hoạt động của hệ thống khi file virus bị loại bỏ bởi phương pháp diệt virus theo cách thông thường không kiểm soát được sự sửa đổi liên kết gốc trong Registry;

Hình 4 thể hiện sơ đồ khối hoạt động của hệ thống thực hiện phương pháp diệt virus máy vi tính loại lây sâu vào hệ thống, theo sáng chế.

Mô tả chi tiết sáng chế

Như đã biết, một hệ điều hành cho máy tính được cấu tạo bởi các file chương trình và chính sự liên kết giữa các file chương trình đó trong hệ thống. Các thông số liên

kết này sẽ được thể hiện trong một cơ sở dữ liệu gọi là Registry đóng vai trò như một bảng liên kết. Trong thực tế trên các hệ điều hành như Microsoft Windows, MAC OS hay Linux thì Registry được lưu trữ trong 1 file hoặc nhiều file. Căn cứ vào bảng liên kết này, hệ điều hành sẽ xác định file nào làm chức năng gì trên hệ thống.

Như được thể hiện trên Hình 1, một hệ thống máy tính thông thường khi cần thực hiện một chức năng, sẽ căn cứ vào các thông số trong Registry (đang trỏ đến file nào) để nạp và thực thi file tương ứng để thực hiện chức năng đó. Ví dụ trong hệ điều hành Windows khi thực hiện chức năng chạy kịch bản đăng nhập khi người sử dụng thực hiện đăng nhập máy vi tính, sẽ căn cứ vào thông số liên kết gốc trong Registry là HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit để xác định sẽ chạy chương trình nào, theo đó sẽ chạy chương trình C:\Windows\System32\Userinit.exe để thực hiện các kịch bản đăng nhập.

Tham khảo Hình 2 , khi hệ thống bị nhiễm virus loại lây sâu vào hệ thống, theo đó virus này sẽ cài đặt thêm file virus vào hệ thống, đồng thời sửa lại thông số liên kết trong Registry để thay vì trỏ đến file gốc của hệ thống, thông số liên kết được sửa để trỏ đến file virus cài đặt thêm vào. Lúc này, hệ thống khi thực hiện chức năng sẽ theo chỉ định của thông số liên kết trong Registry đã bị virus sửa, dẫn tới thay vì nạp và thực thi file gốc ban đầu lại nạp và thực thi file virus trước, sau đó virus mới gọi lại file gốc của hệ thống. Ví dụ trên hệ điều hành Windows, virus loại lây sâu vào hệ thống khi lây nhiễm vào máy vi tính đã cài đặt thêm file virus C:\Windows\Userinit.exe vào hệ thống, sau đó virus này đã sửa thông số liên kết trong Registry là HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit để thông số này thay vì trỏ đến file gốc của hệ thống là C:\Windows\System32\Userinit.exe thì lại trỏ đến file virus cài đặt thêm vào là C:\Windows\Userinit.exe. Dẫn tới lúc này, khi thực hiện kịch bản đăng nhập, hệ thống sẽ theo chỉ định của thông số trong Registry dẫn tới thực thi file của virus là C:\Windows\Userinit.exe trước, sau đó file virus này mới gọi lại file gốc của hệ thống là C:\Windows\System32\Userinit.exe.

Điểm khác biệt của virus loại lây sâu vào hệ thống là chúng tấn công vào mối liên kết giữa các thành phần của hệ điều hành. Trong khi các loại virus lây file (lây vào file chương trình phần mềm hay lây vào file hệ thống) hay lây boot sector thì virus lây nhiễm vào đối tượng cụ thể là file hay boot sector, không tác động tới mối liên kết của đối tượng với các thành phần khác của hệ điều hành.

Tham khảo Hình 3, hoạt động của hệ thống khi file virus bị loại bỏ, trong khi các liên kết không được khôi phục hoặc bị loại bỏ, dẫn tới hệ điều hành và phần mềm tiện ích không hoạt động được bình thường. Các phần mềm diệt virus hiện nay khi diệt virus loại lây sâu vào hệ thống nêu trên chỉ thực hiện việc loại bỏ file virus và/hoặc xóa thông số liên kết trỏ đến file virus mà không khôi phục lại các liên kết gốc của hệ điều hành, dẫn đến sau khi diệt virus, hệ điều hành hoặc phần mềm tiện ích không hoạt động được, do khi thực hiện chức năng, thì không còn thông số liên kết trong Registry vì thông số này bị phần mềm diệt virus loại bỏ khi diệt virus, hoặc còn thông số liên kết trong Registry nhưng vẫn trỏ đến file virus trong khi file virus này đã không còn tồn tại vì đã bị loại bỏ bởi phần mềm diệt virus trước đó. Điều này khiến cho hệ điều hành và phần mềm tiện ích không hoạt động được bình thường như trước khi diệt virus. Ví dụ trên hệ điều hành Windows, trong trường hợp virus sửa đổi thông số liên kết HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit để trỏ đến file virus cài đặt thêm vào là C:\Windows\Userinit.exe, nếu thực hiện loại bỏ file virus C:\Windows\Userinit.exe thì khi hệ điều Windows cần thực hiện kịch bản đăng nhập, hệ điều hành sẽ căn cứ vào thống số liên kết trong Registry đã bị virus sửa đổi nên sẽ tìm và thực thi file virus là C:\Windows\Userinit.exe, tuy nhiên file này đã bị loại bỏ nên không được thực thi, dẫn tới file gốc là C:\Windows\System32\Userinit.exe cũng không được gọi, hệ điều hành không hoạt động được.

Theo sơ đồ thể hiện trên Hình 4, phương pháp diệt virus theo sáng chế sẽ khắc phục tình trạng nêu trên bằng việc khôi phục thông số liên kết gốc từ cơ sở dữ liệu Registry gốc (cơ sở dữ liệu này được phần mềm diệt virus nạp lên khi phát hiện virus trên máy) để ghi đè lên thông số liên kết bị virus sửa đổi. Cơ sở dữ liệu Registry gốc

được xây dựng thông qua thống kê thực nghiệm. Cụ thể bằng cách cài đặt các phiên bản của hệ điều hành trên máy vi tính rồi tiến hành thống kê tất cả các file hệ thống là file thực thi có trong thư mục hệ thống của hệ điều hành. Sau đó duyệt toàn bộ bảng Registry để tìm các thông số liên kết trỏ đến các file hệ thống đã được thống kê nói trên, nếu tìm thấy sẽ sao chép lại thông số liên kết tìm được để lập thành cơ sở dữ liệu Registry gốc. Việc thống kê thực nghiệm theo cách này được thực hiện dễ dàng vì cùng một phiên bản hệ điều hành, khi cài lên các máy tính khác nhau sẽ cho ra cùng các file hệ thống và cùng bảng Registry có giá trị giống nhau.

Ví dụ như với hệ điều hành Microsoft Windows, file userinit.exe là một file hệ thống, vì file này là file thực thi nằm trong thư mục System32 của hệ thống. File userinit.exe này sẽ được thống kê lại trong danh sách file hệ thống. Khi duyệt bảng Registry sẽ thấy thông số liên kết HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit trỏ đến file userinit.exe kể trên, do đó, thông số liên kết HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit sẽ được sao chép để đưa vào cơ sở dữ liệu Registry gốc cho hệ điều hành Microsoft Windows. Làm tương tự với các file hệ thống khác để thu được cơ sở dữ liệu Registry gốc của hệ điều hành.

Trong bản mô tả sáng chế này, "Virus loại lây sâu vào hệ thống" là loại virus có khả năng chống lại việc loại bỏ chúng ra khỏi hệ thống bằng cách chúng đăng ký và cài đặt lại các thông số liên kết trong Registry khiến cho khi các phần mềm diệt virus loại bỏ file virus trong khi các liên kết không được khôi phục, sẽ làm cho hệ điều hành hoặc phần mềm tiện ích không còn hoạt động hoặc không hoạt động một cách bình thường như trước khi diệt virus.

Trong bản mô tả sáng chế này, "Môđun nhận diện" được hiểu là một đoạn chương trình trong phần mềm hoặc một phần mềm có sẵn chức năng nhận diện virus theo cách thông thường.

Trong bản mô tả sáng chế này, "Mô đun xử lý virus thông thường" được hiểu là một đoạn chương trình trong phần mềm hoặc một phần mềm có sẵn chức năng diệt virus thông thường.

Trong bản mô tả sáng chế này, "Cơ sở dữ liệu Registry gốc" được hiểu là cơ sở dữ liệu của Registry gốc được lưu trữ sẵn trong file dữ liệu của phần mềm diệt virus để phục vụ mục đích tra cứu khi diệt virus

Trong bản mô tả sáng chế này, "Liên kết cần hiệu chỉnh" là liên kết đã bị virus loại lây sâu vào hệ thống sửa đổi giá trị để thay vì trỏ đến file gốc của hệ thống, liên kết này lại trỏ đến file virus cài đặt thêm vào.

Trong bản mô tả sáng chế này, "liên kết gốc" là liên kết ban đầu của hệ điều hành trước khi bị virus loại lây sâu vào hệ thống sửa đổi.

Theo HÌNH 4, sơ đồ hoạt động của phương pháp diệt virus máy vi tính loại lây sâu vào hệ thống không làm ảnh hưởng đến hoạt động bình thường của hệ điều hành được thực hiện theo các bước như sau:

(1) Môđun nhận diện virus tiến hành kiểm tra các file đang hoạt động trên hệ điều hành, kiểm tra xem có file nào nhiễm virus không. Nếu không có file virus thì kết thúc quy trình diệt virus, nếu có file virus thì chuyển sang bước (2).

(2) Kiểm tra trong Registry xem có liên kết nào trỏ tới file virus đang được kiểm tra này không. Nếu không có liên kết nào trỏ tới file virus này thì xác định đây là loại virus thông thường và điều khiển chuyển sang môđun xử lý virus thông thường. Nếu có liên kết trỏ tới file virus này, thì xác định đây là liên kết cần hiệu chỉnh và chuyển sang bước (3).

(3) Thực hiện loại bỏ file virus, sau đó tiếp tục chuyển sang bước (4).

(4) Nạp cơ sở dữ liệu Registry gốc từ file lên bộ nhớ, hiệu chỉnh lại liên kết cần hiệu chỉnh về thông số liên kết gốc của hệ điều hành, để liên kết này không trỏ đến file virus

nữa và chuyển sang trỏ tới file gốc của hệ điều hành. Cụ thể lấy giá trị của liên kết gốc từ cơ sở dữ liệu Registry gốc để ghi đè lên liên kết cần hiệu chỉnh.

(5) Kết thúc xử lý. Quá trình diệt virus được hoàn tất.

Ưu điểm của phương pháp diệt virus máy vi tính theo sáng chế như nêu trong bản mô tả này bao gồm các bước như nêu trên là đảm bảo được sự hoạt động bình thường của hệ điều hành khi kết thúc việc diệt virus.

YÊU CẦU BẢO HỘ

1. Phương pháp diệt virus máy vi tính loại lây sâu vào hệ thống không làm ảnh hưởng đến hoạt động bình thường của hệ điều hành bao gồm các bước:

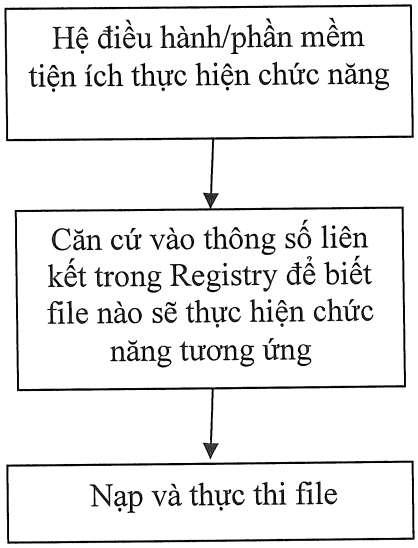
(i) kiểm tra xem file có phải file virus bằng đoạn chương trình trong phần mềm hoặc một phần mềm có sẵn chức năng nhận diện virus theo cách thông thường; nếu là file virus thì chuyển sang bước (ii);

(ii) kiểm tra trong Registry xem có liên kết nào trỏ tới file virus không; nếu có chuyển sang bước (iii);

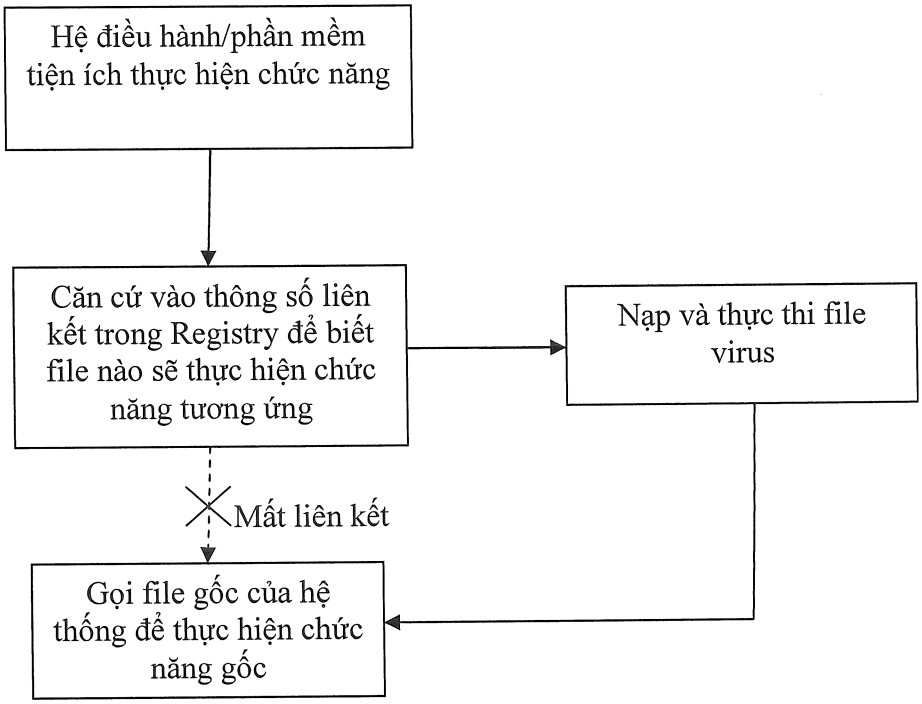
(iii) loại bỏ file virus; chuyển sang bước (iv);

(iv) hiệu chỉnh lại liên kết đang trỏ tới file virus, khôi phục lại liên kết gốc từ cơ sở dữ liệu Registry gốc bằng cách ghi đè liên kết gốc lên liên kết bị sửa đổi, nhờ đó liên kết không trỏ đến file virus nữa và chuyển sang trỏ tới file gốc của hệ điều hành;

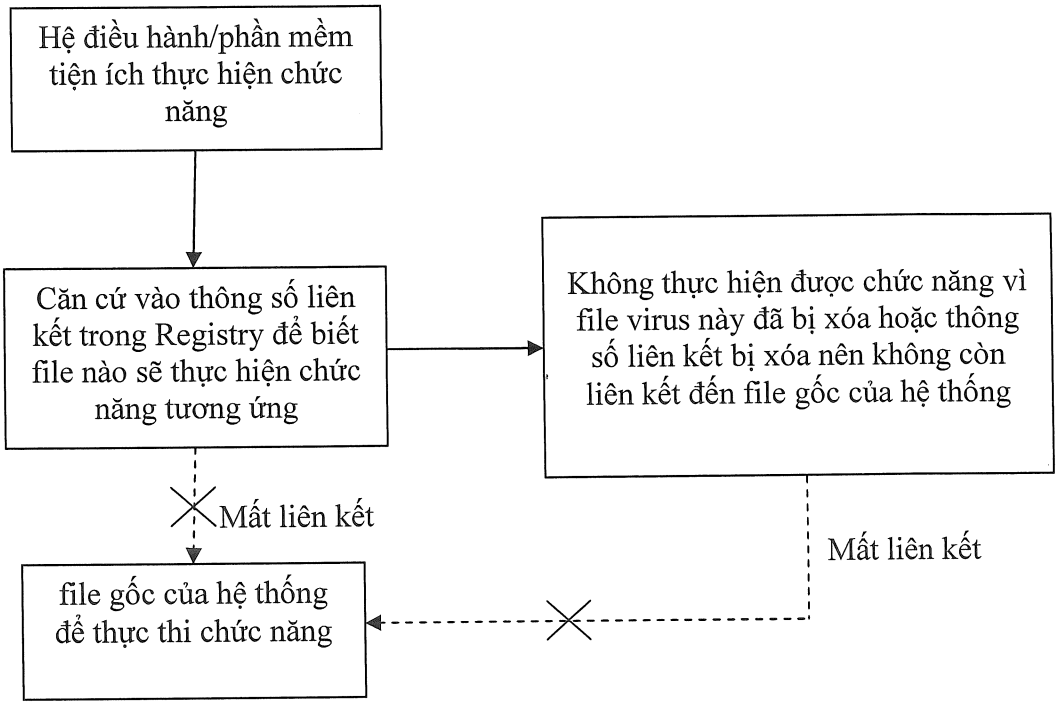
HÌNH 1


Hệ điều hành/phần mềm tiện ích thực hiện chức năng
Căn cứ vào thông số liên kết trong Registry để biết file nào sẽ thực hiện chức năng tương ứng
Nạp và thực thi file

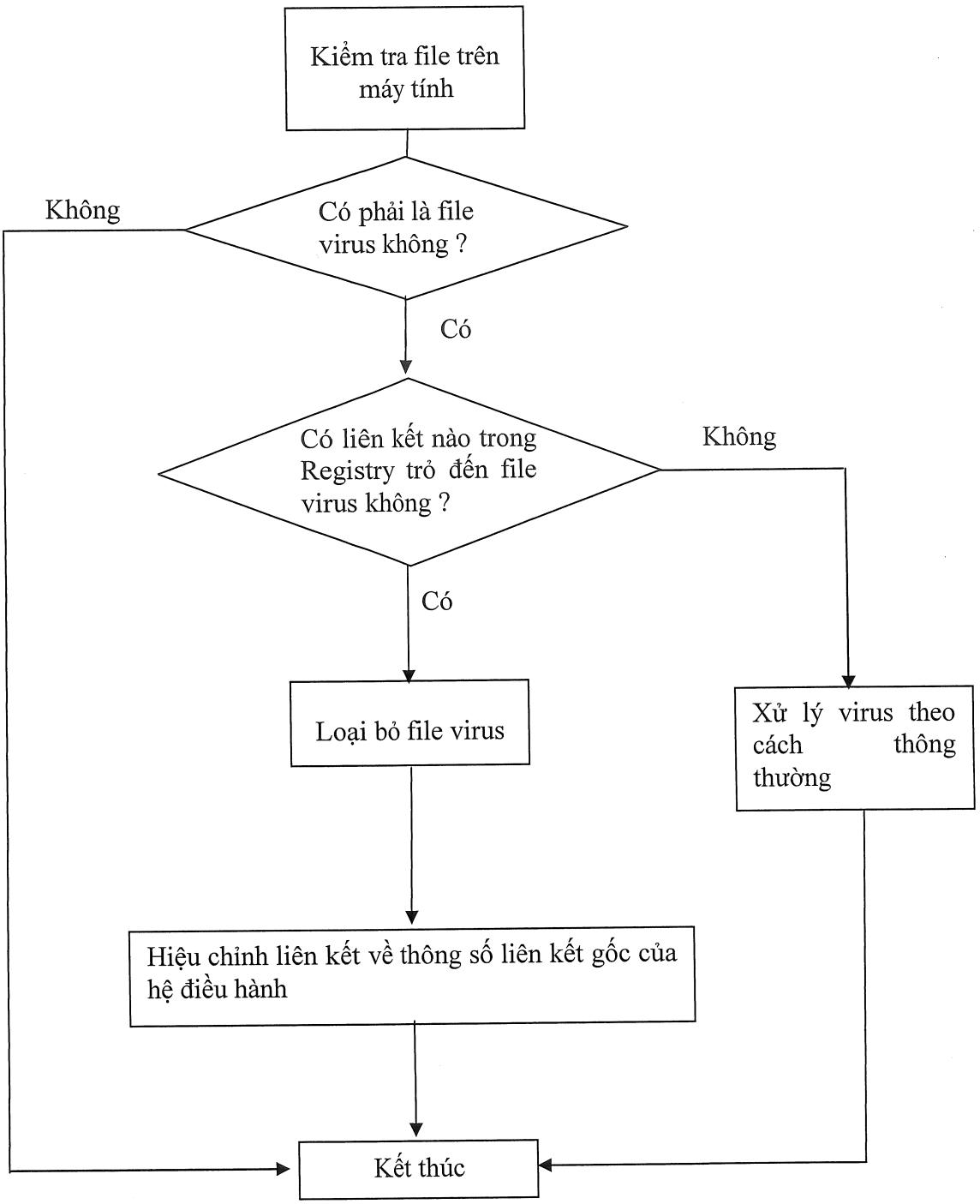
HÌNH 2


Hệ điều hành/phần mềm tiện ích thực hiện chức năng
Căn cứ vào thông số liên kết trong Registry để biết file nào sẽ thực hiện chức năng tương ứng
Nạp và thực thi file virus
Mất liên kết
Gọi file gốc của hệ thống để thực hiện chức năng gốc

HÌNH 3


Hệ điều hành/phần mềm tiện ích thực hiện chức năng
Căn cứ vào thông số liên kết trong Registry để biết file nào sẽ thực hiện chức năng tương ứng
Không thực hiện được chức năng vì file virus này đã bị xóa hoặc thông số liên kết bị xóa nên không còn liên kết đến file gốc của hệ thống
Mất liên kết
Mất liên kết
file gốc của hệ thống để thực thi chức năng

HÌNH 4


Kiểm tra file trên máy tính
Có phải là file virus không ?
Không
Có
Có liên kết nào trong Registry trỏ đến file virus không ?
Không
Có
Loại bỏ file virus
Xử lý virus theo cách thông thường
Hiệu chỉnh liên kết về thông số liên kết gốc của hệ điều hành
Kết thúc