ỦY BAN NHÂN DÂN TỈNH CAO BẰNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 988 /KH-UBND	*Cao Bằng, ngày 25 tháng 4 năm 2023*

KẾ HOẠCH
Triển khai rà quét, xử lý, bóc gỡ mã độc các hệ thống thông tin tại cơ quan nhà nước trên địa bàn tỉnh Cao Bằng năm 2023

Thực hiện Kế hoạch số 205/KH-UBND ngày 02/02/2023 của Ủy ban nhân dân tỉnh Cao Bằng về Triển khai thực hiện Quyết định số 964/QĐ-TTg ngày 10 tháng 8 năm 2022 của Thủ tướng chính phủ phê duyệt "Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030" trên địa bàn tỉnh Cao Bằng, Ủy ban nhân dân (UBND) tỉnh ban hành Kế hoạch rà quét, xử lý, bóc gỡ mã độc các hệ thống thông tin tại cơ quan nhà nước trên địa bàn tỉnh năm 2023 như sau:

I. MỤC ĐÍCH, YÊU CẦU

- Triển khai thực hiện rà quét, xử lý mã độc cho các hệ thống thông tin tại các cơ quan Nhà nước trên địa bàn tỉnh; bảo đảm 100% máy chủ, máy trạm, các thiết bị đầu cuối tại các cơ quan, đơn vị trên địa bàn tỉnh có giải pháp phòng, chống mã độc bảo vệ và có cơ chế tự động cập nhật phiên bản mới hoặc dấu hiệu nhận dạng mã độc mới.

- Kịp thời nâng cao nhận thức cho cán bộ, công chức, viên chức, người lao động trong cơ quan nhà nước về tầm quan trọng của bảo đảm an toàn thông tin trên không gian mạng; thúc đẩy việc chấp hành nghiêm về chủ trương, đường lối, các quy định của Đảng, chính sách pháp luật của nhà nước liên quan đến an toàn thông tin.

- Hoạt động rà quét, xử lý bóc gỡ mã độc không làm xáo trộn, không gây cản trở, ảnh hưởng đến công việc chuyên môn của các phòng, ban tại cơ quan, đơn vị, địa phương.

II. NỘI DUNG THỰC HIỆN

1. Công tác chỉ đạo, triển khai thực hiện các quy định bảo đảm an toàn thông tin

- Chỉ đạo, quán triệt, triển khai thực hiện các văn bản, quy định về công tác bảo đảm an toàn thông tin mạng, như: Luật An toàn thông tin mạng năm 2018; Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về nâng cao năng lực phòng chống phần mềm độc hại; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số

85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ...

- Tổ chức tuyên truyền, phổ biến, tập huấn nhằm nâng cao nhận thức, kỹ năng xử lý các mối nguy hại của mã độc và trách nhiệm của các đơn vị, tổ chức, cá nhân trong công tác phòng, chống mã độc của các hệ thống thông tin trong phạm vi đơn vị.

- Tổ chức rà soát, kiểm tra, đánh giá về an toàn thông tin cho các hệ thống thông tin tại đơn vị theo quy định tại Nghị định số 85/2016/NĐ-CP của Chính phủ và Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông; xây dựng, ban hành phương án, kịch bản ứng cứu sự cố cho các hệ thống thông tin do cơ quan, đơn vị quản lý và cập nhật kịp thời khi có thay đổi.

2. Công tác rà quét, xử lý bóc gỡ mã độc

- Tập trung vận hành ổn định Hệ thống quản lý phòng, chống mã độc tập trung và kết nối về Trung tâm Giám sát An toàn không gian mạng quốc gia thuộc Cục An toàn thông tin - Bộ Thông tin và Truyền thông.

- Tổ chức thực hiện các giải pháp phòng, chống mã độc, bảo vệ 100% máy chủ, máy trạm và thiết bị đầu cuối theo hướng dẫn của Sở Thông tin và Truyền thông.

- Thực hiện rà quét máy tính, thiết bị bằng phần mềm phòng chống mã độc đang có hoặc các công cụ khuyến nghị *(thực hiện theo Hướng dẫn tại Phụ lục I kèm theo Kế hoạch này).*

3. Thời gian thực hiện: Trong tháng 5 và tháng 6 năm 2023.

III. TỔ CHỨC THỰC HIỆN

1. Sở Thông tin và Truyền thông

- Chủ trì, phối hợp với Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Cục An toàn Thông tin - Bộ Thông tin và Truyền thông kiểm tra, đảm bảo thông tin kết nối, chia sẻ dữ liệu mã độc.

- Theo dõi, đôn đốc, hướng dẫn, hỗ trợ các đơn vị trong quá trình thực hiện các nội dung tại Kế hoạch.

- Tổng hợp, báo cáo kết quả thực hiện về UBND tỉnh trước **ngày 30/6/2023**.

2. Các Sở, Ban ngành, UBND các huyện, thành phố

- Tổ chức quán triệt cán bộ, công chức, viên chức, người lao động trong cơ quan, đơn vị, địa phương nâng cao nhận thức về bảo đảm an toàn thông tin trên không gian mạng.

- Xây dựng, hoàn thiện hồ sơ đề xuất cấp độ các hệ thống thông tin thuộc phạm vi quản lý, gửi về Sở Thông tin và Truyền thông để thẩm định, phê duyệt hoặc trình cấp có thẩm quyền phê duyệt theo quy định.

- Xây dựng quy chế bảo đảm an toàn hệ thống thông tin cho hệ thống đáp ứng các yêu cầu an toàn về quản lý theo cấp độ an toàn hệ thống thông tin tương ứng.

- Ban hành phương án, kịch bản ứng cứu sự cố cho các hệ thống thông tin do cơ quan, đơn vị quản lý.

- Thực hiện rà quét, xử lý, bóc gỡ mã độc và báo cáo kết quả thực hiện về Sở Thông tin và Truyền thông trước **ngày 25/6/2023** *(theo mẫu tại Phụ lục 2 kèm theo Kế hoạch này).*

Trên đây là Kế hoạch triển khai rà quét, xử lý bóc gỡ mã độc trong cơ quan nhà nước trên địa bàn tỉnh Cao Bằng năm 2023; yêu cầu các Sở, Ban ngành, UBND các huyện, thành phố triển khai thực hiện. Trong quá trình thực hiện nếu có khó khăn, vướng mắc, các cơ quan, địa phương phản ánh về UBND tỉnh (qua Sở Thông tin và Truyền thông) để tổng hợp, chỉ đạo giải quyết./.

Nơi nhận:
- Cục An toàn thông tin - Bộ TT&TT;
- Chủ tịch, các PCT UBND tỉnh;
- Các Sở, Ban, ngành;
- UBND các huyện, thành phố;
- VP UBND tỉnh: CVP, PCVP *(Huyền)*; TTTT, TTPVHCC, TP.VX;
- Lưu: VT, VX(M).

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Trịnh Trường Huy

Phụ lục 1

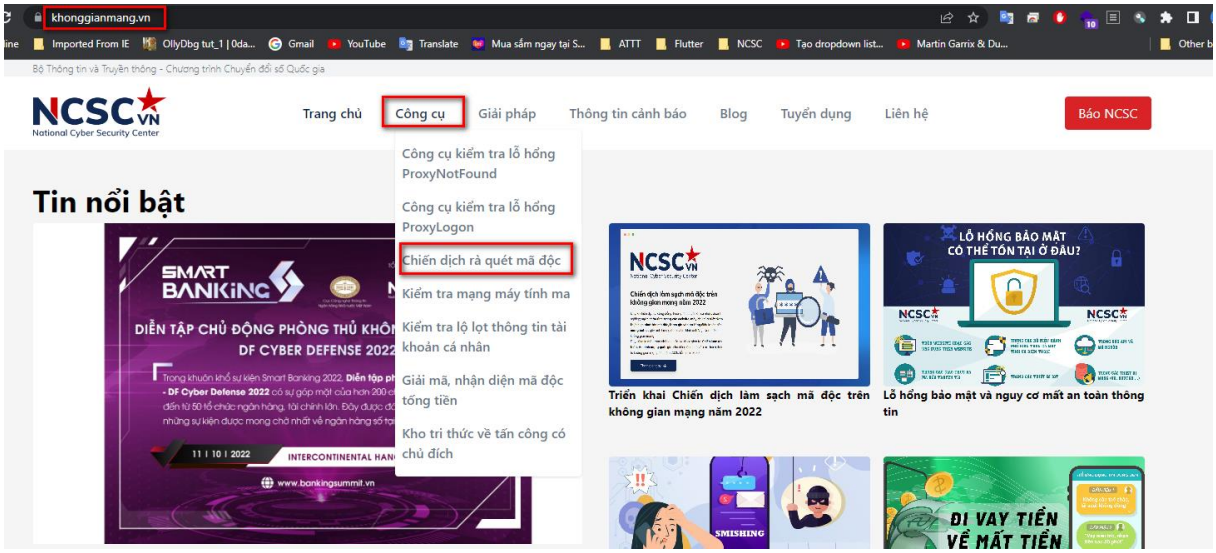
HƯỚNG DẪN RÀ QUÉT, BÓC GỠ MÃ ĐỘC

(Kèm theo Kế hoạch số 988 /KH-UBND ngày 25/4/2023 của UBND tỉnh Cao Bằng)

1. Sử dụng công cụ: Chiến dịch rà quét mã độc

Bước 1: Truy cập địa chỉ https://khonggianmang.vn

Bước 2: Nhấp chuột vào tag "**Công cụ**" -> Chọn "**Chiến dịch rà quét mã độc**"



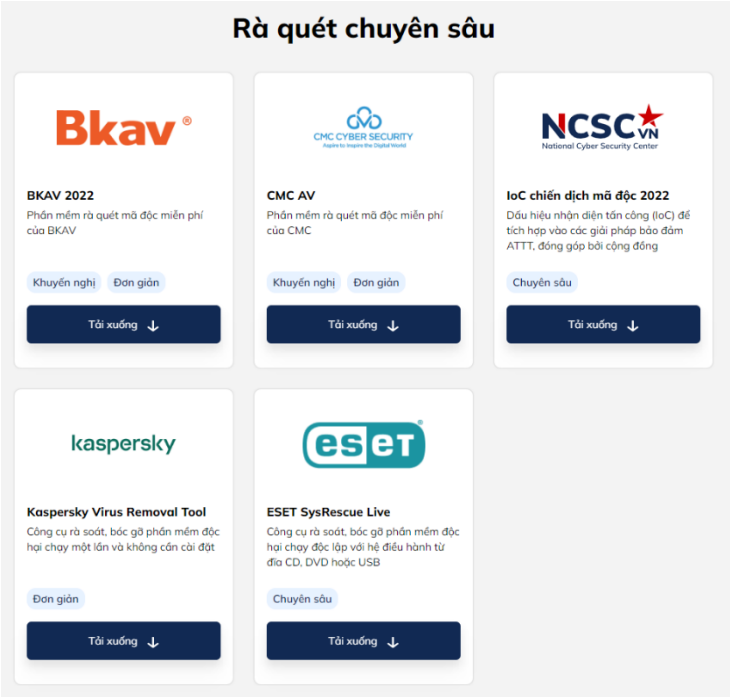
Bước 3: thực hiện rà quét mức mạng

Kết quả rà soát mức mạng

TIÊU CHÍ KIỂM TRA	KẾT QUẢ	
Địa chỉ IP	1[redacted]	AS45899 VNPT Corp - Hanoi
Hệ điều hành	**Windows 10**	Hệ điều hành của bạn an toàn
Trình duyệt	**Chrome 111.0.0.0**	Trình duyệt của bạn an toàn
Lộ lọt dữ liệu	**Chưa phát hiện lộ lọt**	Không ghi nhận lộ lọt dữ liệu trong 30 ngày qua
Nằm trong mạng máy tính độc hại	**Không**	Không ghi nhận kết nối tới mạng máy tính độc hại trong 30 ngày qua

Bước 4: Rà quét chuyên sâu bằng phần mềm phòng chống mã độc đang có hoặc các công cụ khuyến nghị. *(Trường hợp đã cài đặt phần mềm Bitdefender theo công văn 740/STTTT-TTCNTTTT thì không cần thực hiện bước này).*

Chú ý chỉ nên cài đặt và chạy 01 ứng dụng

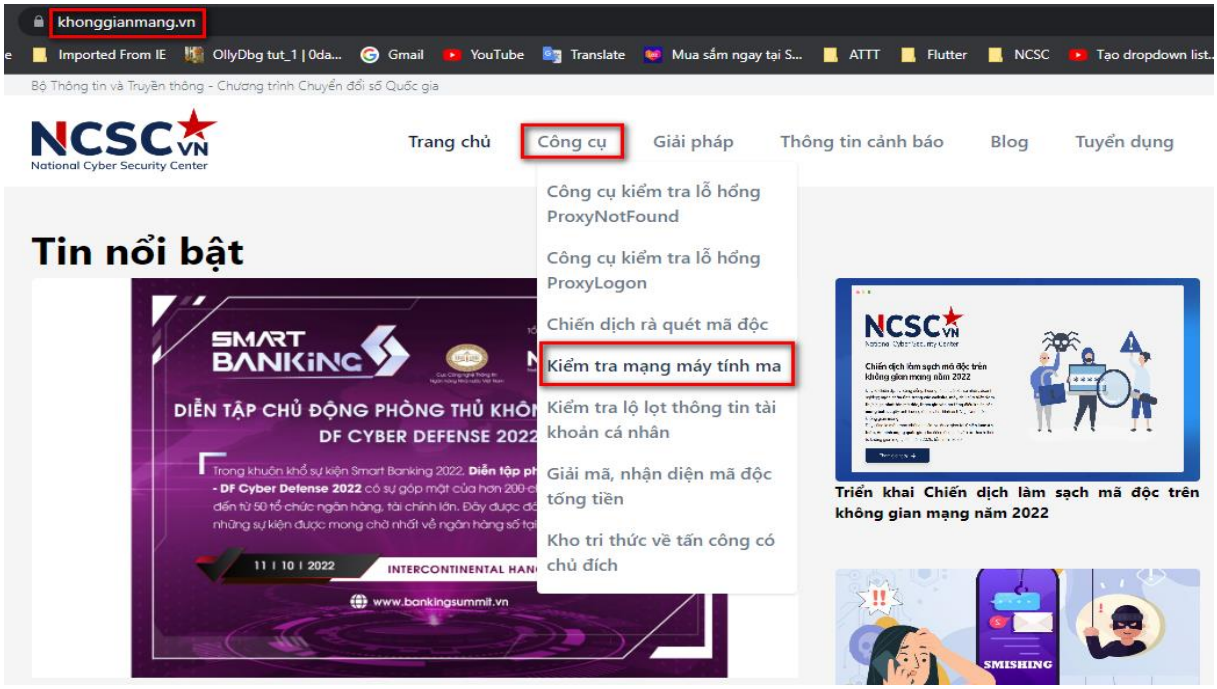


Bước 5: Kiểm tra kết quả.

2. Công cụ: Kiểm tra mạng máy tính ma

Công cụ Kiểm tra mạng máy tính ma giúp người dùng, tổ chức kiểm tra xem địa chỉ IP của mình có liên quan đến mã độc hay không, từ đó có phương án để xử lý kịp thời.

Bước 1: Từ trang chủ của khonggianmang.vn, chọn tag "**Công cụ**" -> Chọn "**Kiểm tra mạng máy tính ma**".



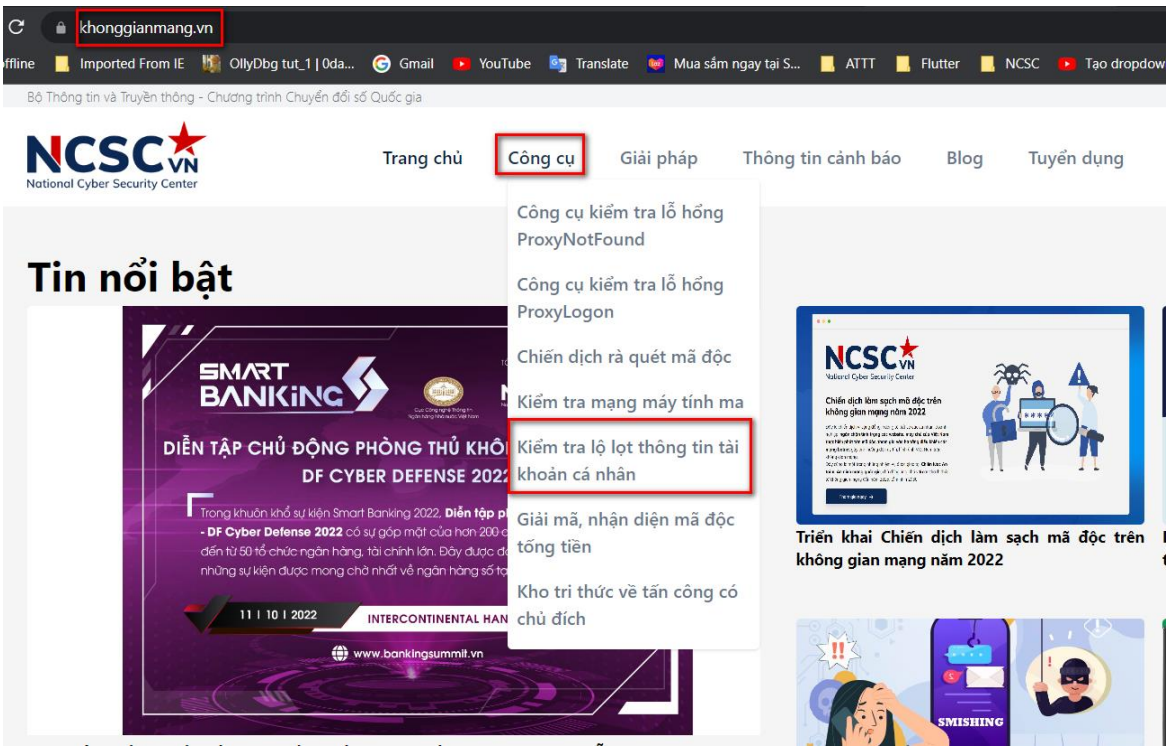
Bước 2: Chọn "**Kiểm tra ngay**".

Bước 3: Kiểm tra kết quả.

3. Công cụ: Kiểm tra lộ lọt thông tin tài khoản trực tuyến

Công cụ Kiểm tra lộ lọt thông tin tài khoản trực tuyến hỗ trợ việc kiểm tra thông tin tài khoản email có bị lộ lọt trên mạng không, để hỗ trợ người dùng kịp thời phòng tránh các cuộc tấn công có thể xảy ra.

Bước 1: Từ trang chủ của **khonggianmang.vn**, chọn tag "**Công cụ**" -> Chọn "**Kiểm tra lộ lọt thông tin tài khoản cá nhân**".



Bước 2: Nhập địa chỉ Email và chọn "**Kiểm tra**".

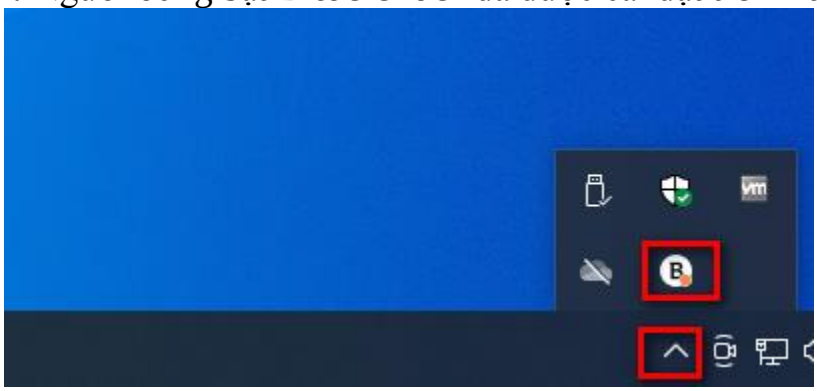
Kết quả đưa ra là "**An toàn**" nếu địa chỉ email không nằm trong danh sách các địa chỉ email bị lộ lọt thông tin của **khonggianmang.vn**

4. Sử dụng các phần mềm Antivirus

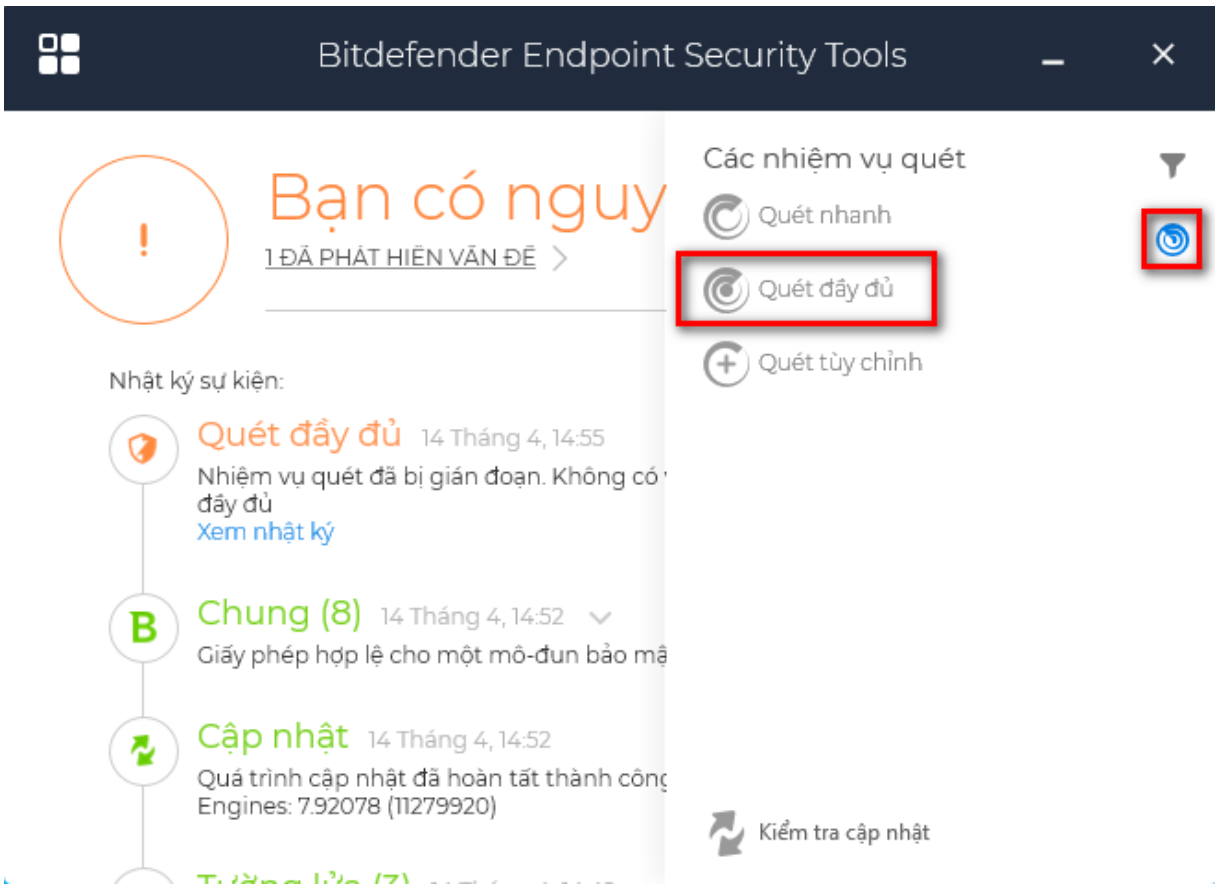
Lưu ý: Chỉ cần cài đặt và sử dụng 01 phần mềm trên máy tính

4.1. Sử dụng phần mềm Bitdefender theo công văn số 740/STTTT-TTCNTTTT

Bước 1: Người dùng bật **Bitdefender** đã được cài đặt trên máy tính

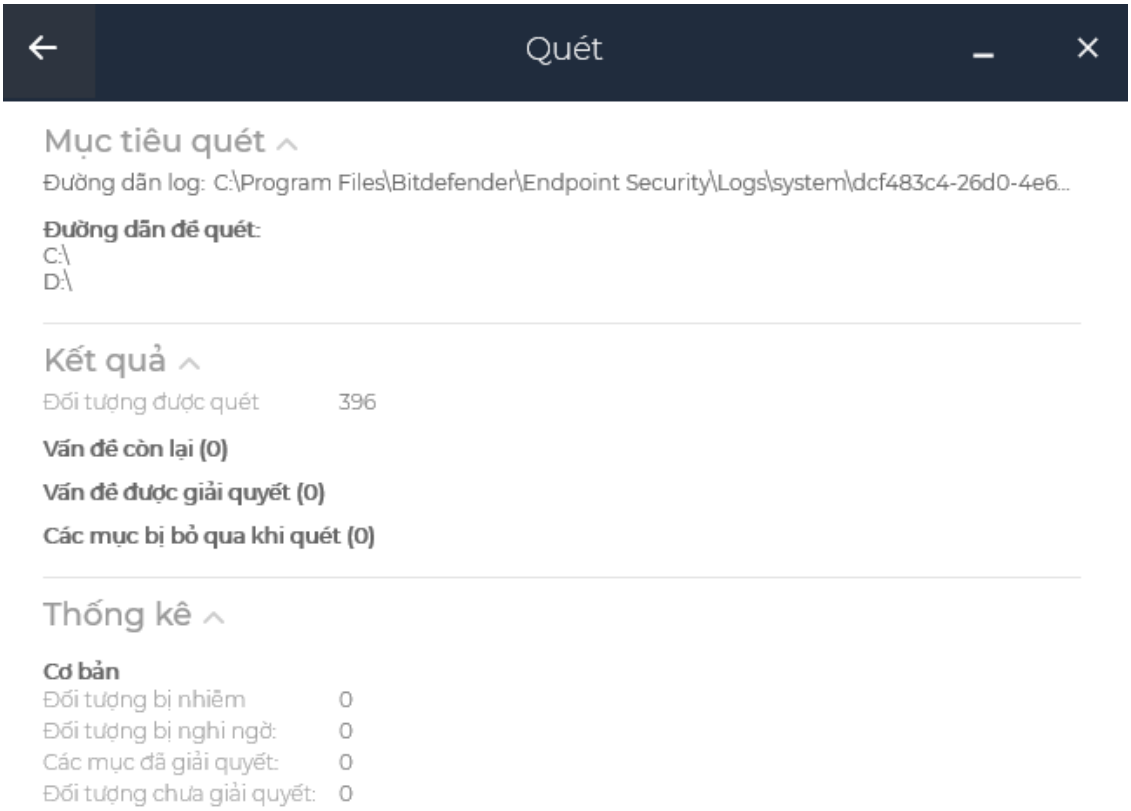


Bước 2: Chọn "**Các nhiệm vụ quét**" , "**Quét đầy đủ**"



Bước 3: Sau khi quét xong, chọn "**Xem nhật ký**" để xem kế quả sau khi quét xong

Kết quả hiển thị



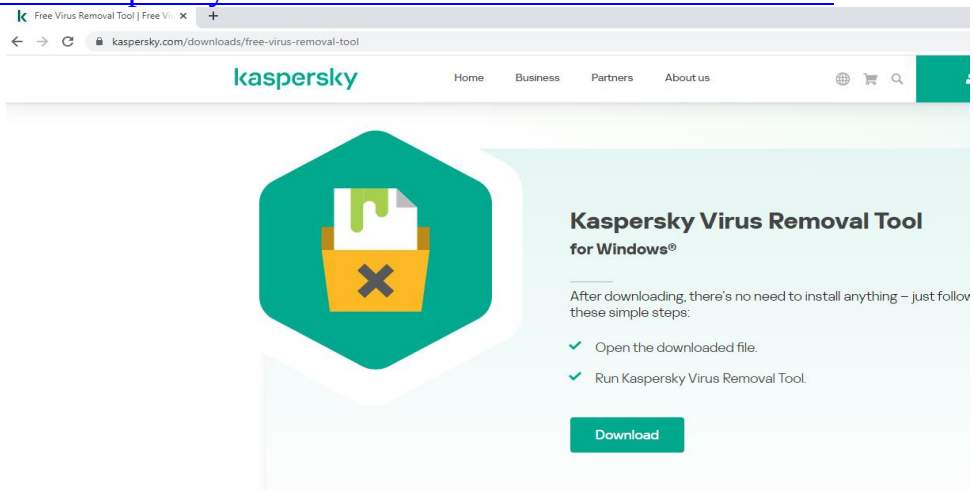
4.2. Sử dụng phần mềm Kaspersky Virus Removal Tool

Kaspersky Virus Removal Tool là một ứng dụng được Kaspersky Lab thiết kế với mục đích trở thành một máy quét virus và được cung cấp hoàn toàn miễn phí bởi Kaspersky. Ứng dụng sẽ phát hiện và gỡ bỏ những phần mềm độc hại, phần mềm gián điệp, virus, trojan, rootkit trên máy tính.

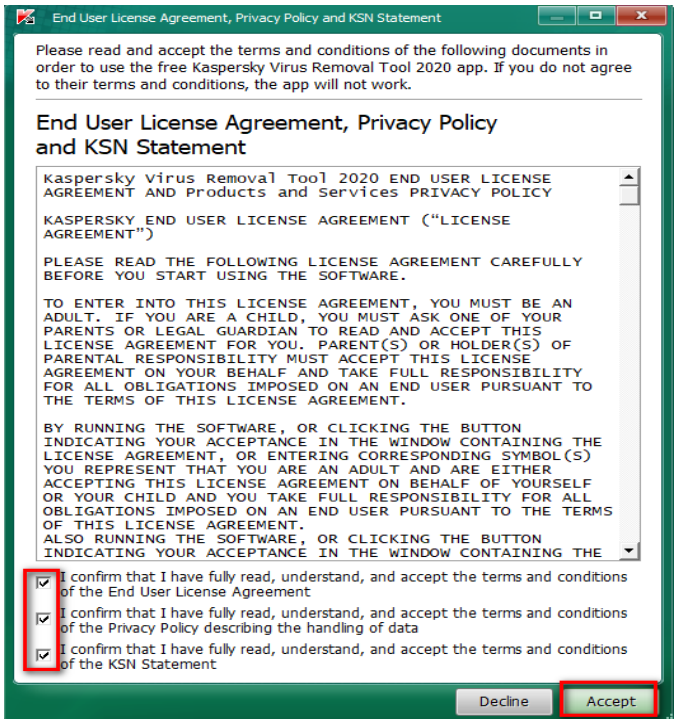
Lưu ý: ứng dụng chỉ quét, gỡ bỏ mã độc khi được người dùng kích hoạt sử dụng, ứng dụng không bảo vệ thời gian thực.

Bước 1: Người dùng tải phần mềm tại địa chỉ

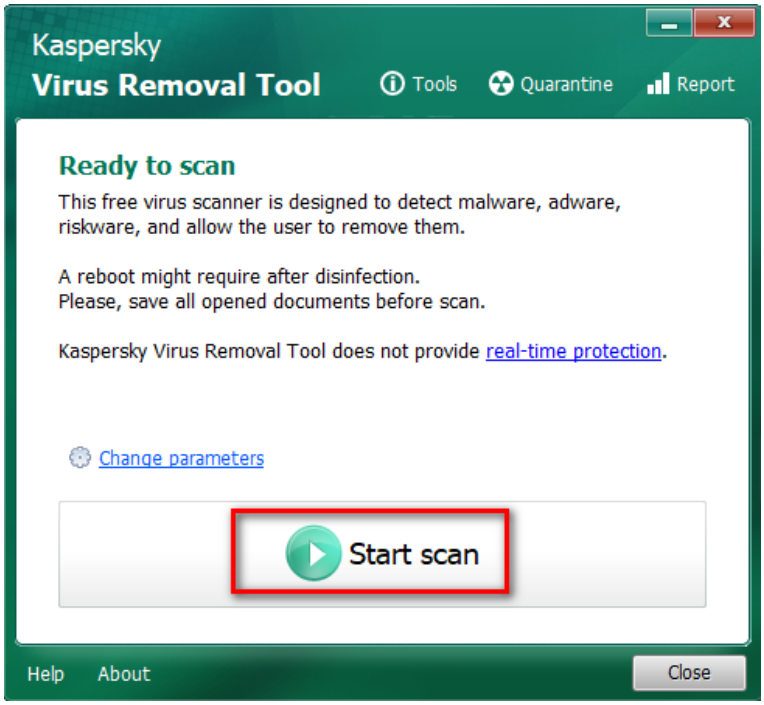
https://www.kaspersky.com/downloads/free-virus-removal-tool



Bước 2: Chạy ứng dụng **KVRT.exe**. Tích chọn đồng ý với điều khoản sử dụng và chọn "**Accept**"

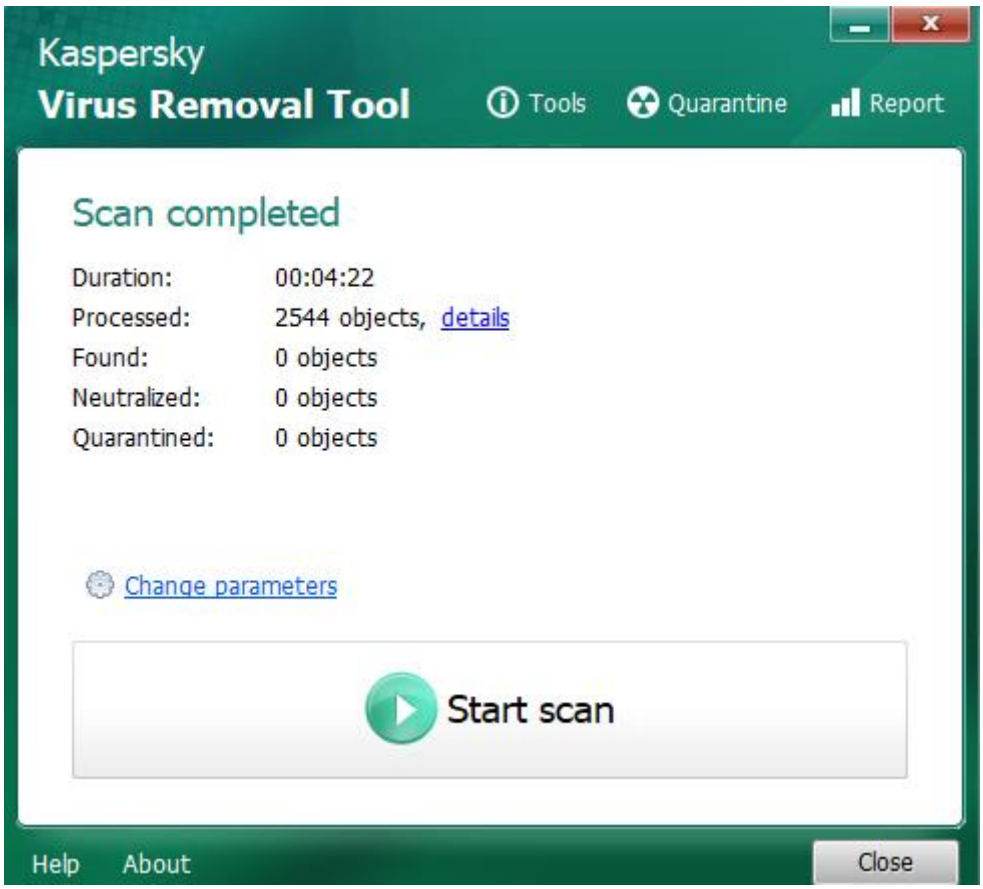


Bước 3: Chọn "**Start scan**" để rà quét mã độc trên hệ thống



Một vài trường hợp có mã độc, ứng dụng yêu cầu khởi động lại máy tính để diệt mã độc, người sử dụng thực hiện theo các thao tác của ứng dụng đưa ra.

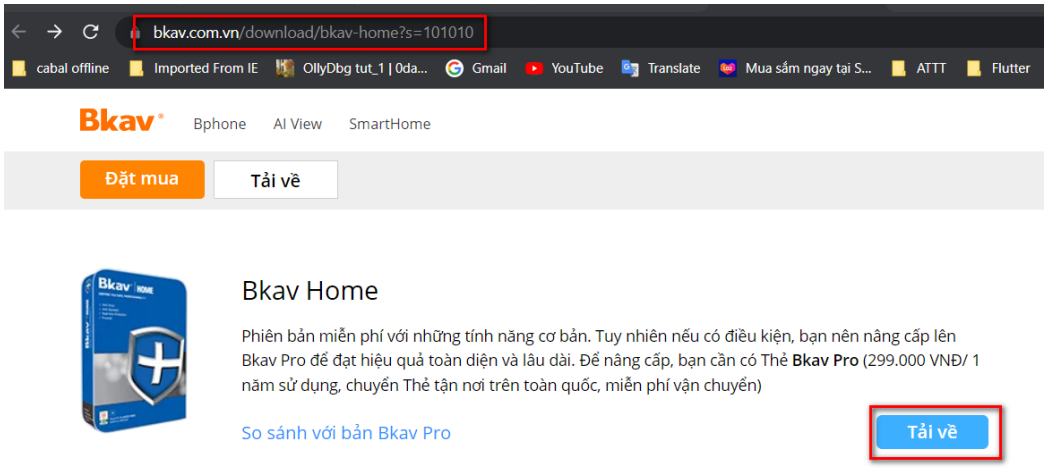
Bước 4: Xem kết quả sau khi rà quét



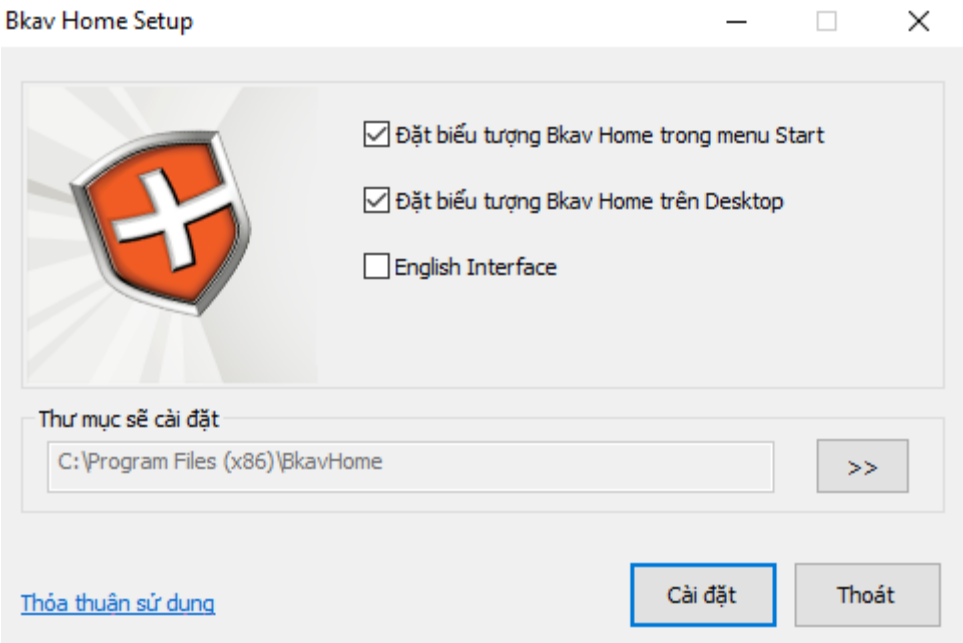
4.3. Sử dụng phần mềm BKAV

Bkav Home là Phần mềm rà quét mã độc miễn phí của BKAV.

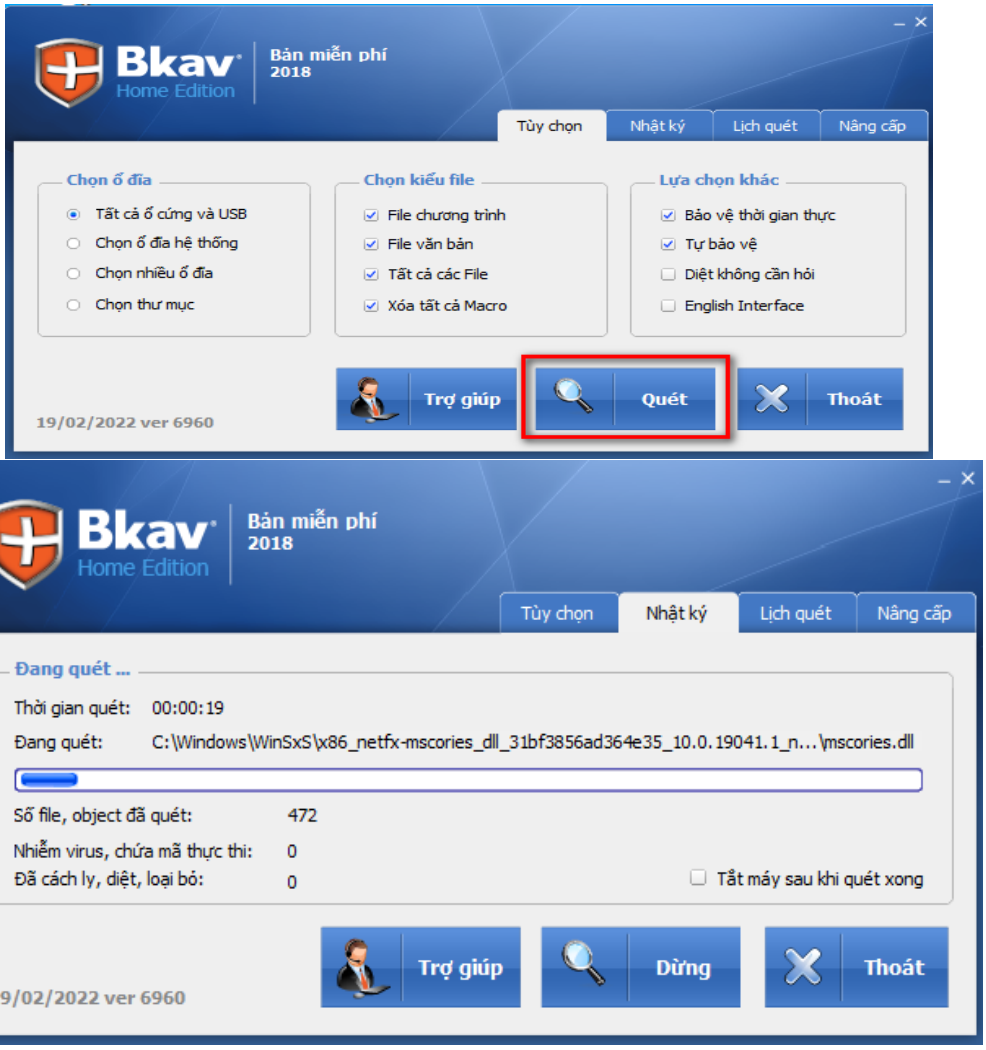
Bước 1: Người dùng tải phần mềm tại địa chỉ https://www.bkav.com.vn/download/bkav-home?s=101010



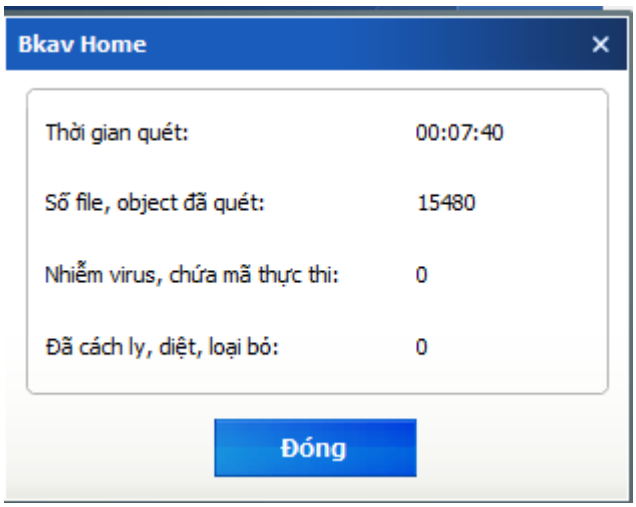
Bước 2: Người dùng cài đặt ứng dụng BKAV từ file đã tải về



Bước 3: Chạy ứng dụng và quét mã độc



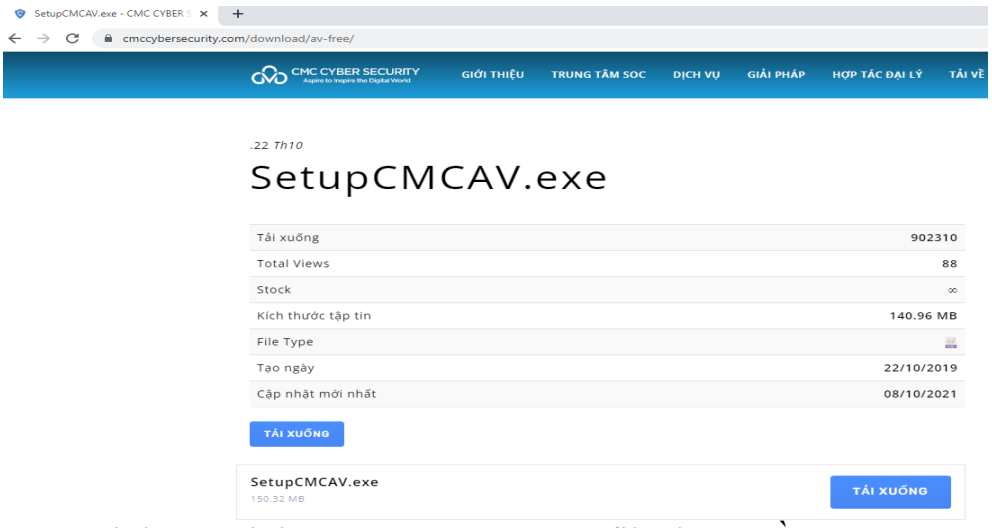
Bước 4: Xem kết quả



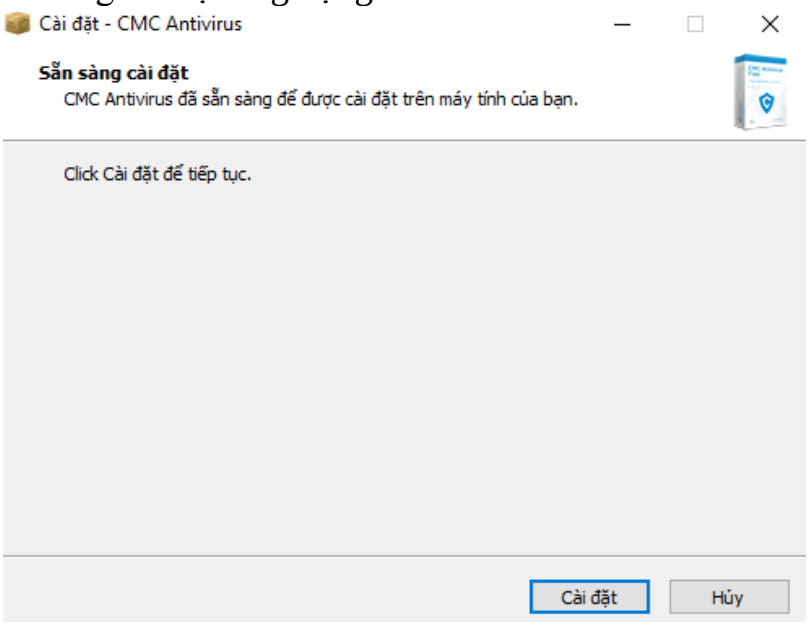
4.3. Sử dụng phần mềm CMC AV

Phần mềm rà quét mã độc miễn phí của CMC

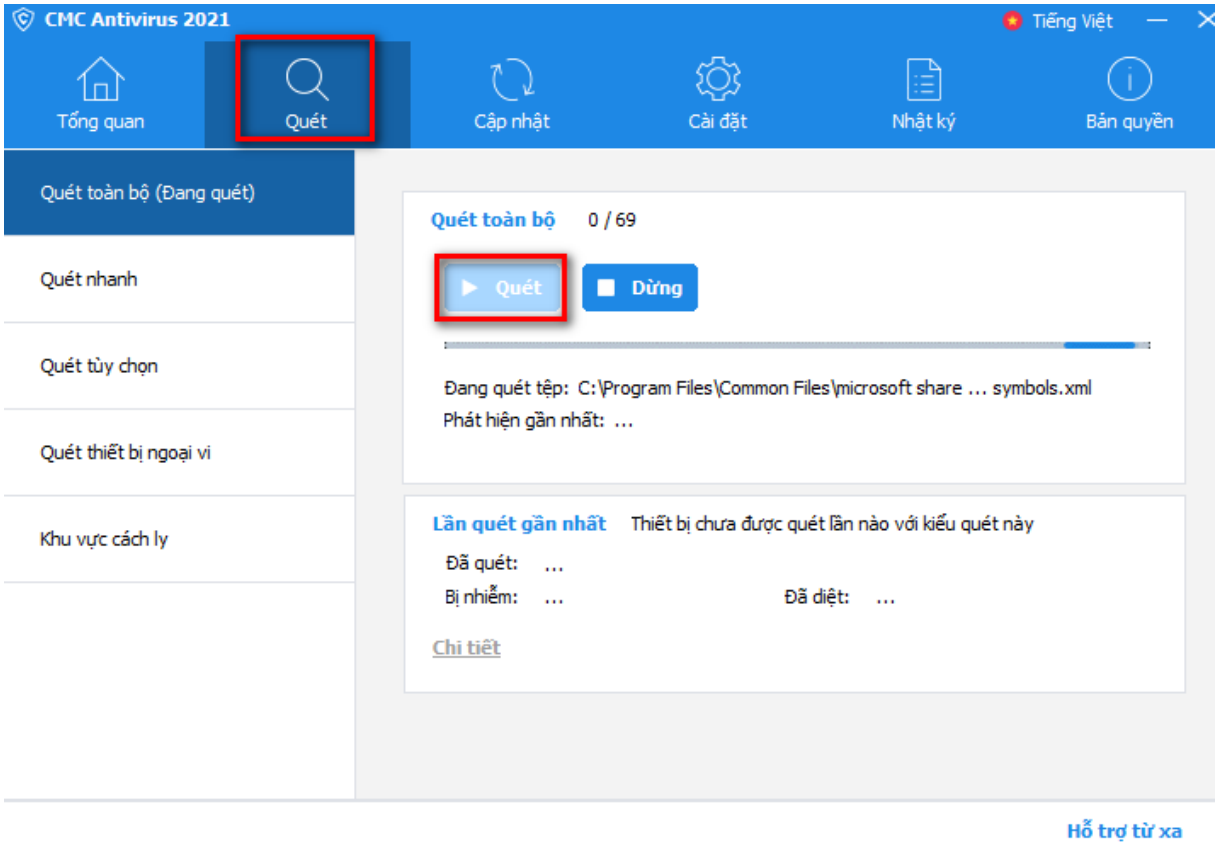
Bước 1: Người dùng tải phần mềm tại địa chỉ https://cmccybersecurity.com/download/av-free/



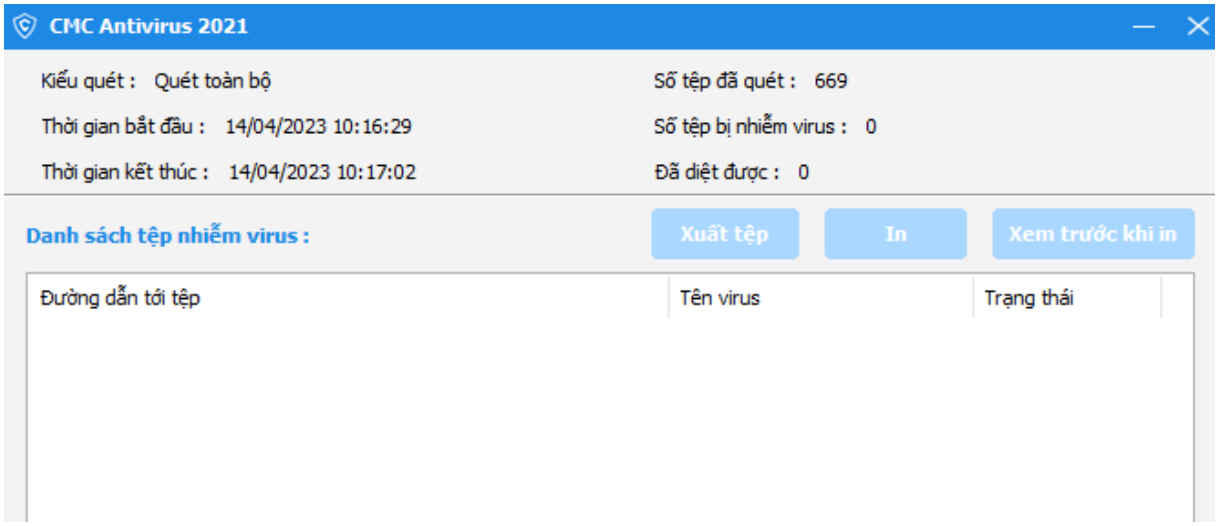
Bước 2: Người dùng cài đặt ứng dụng CMC từ file đã tải về



Bước 3: Chạy ứng dụng và quét mã độc



Bước 4: Xem kết quả



Phụ lục 2
MẪU BÁO CÁO KẾT QUẢ THỰC HIỆN
(Kèm theo Kế hoạch số 988/KH-UBND ngày 25/4/2023 của UBND tỉnh Cao Bằng)

BÁO CÁO
Kết quả triển khai rà quét, xử lý bóc gỡ mã độc tại các cơ quan, đơn vị trên địa bàn tỉnh Cao Bằng năm 2023

1. Thông tin chung:

- Tên đơn vị: .....
- Tên cán bộ cung cấp thông tin:.....
- Số điện thoại: ..... Email: ……

2. Thông tin số liệu:

2.1. Về hồ sơ đề xuất cấp độ theo Nghị định số 85/2016/NĐ-CP:

- Số lượng hệ thống thông tin đã xây dựng hồ sơ đề xuất cấp độ[1] trên tổng số hệ thống thông tin thuộc phạm vi quản lý:.....
- Khó khăn, vướng mắc (nếu có): .....
- Đề xuất, kiến nghị (nếu có): .....

2.2. Ban hành phương án, kịch bản ứng cứu sự cố:

- Đơn vị đã ban hành phương án, kịch bản ứng cứu sự cố[2]: .....
- Khó khăn, vướng mắc (nếu có): .....
- Đề xuất, kiến nghị (nếu có): .....

2.3. Quy chế bảo đảm an toàn hệ thống thông tin cho hệ thống đáp ứng các yêu cầu an toàn về quản lý theo cấp độ an toàn hệ thống thông tin tương ứng

- Đơn vị đã ban hành Quy chế bảo đảm an toàn hệ thống thông tin cho hệ thống[3] trên tổng số hệ thống thông tin thuộc phạm vi quản lý: .....
- Khó khăn, vướng mắc (nếu có): .....
- Đề xuất, kiến nghị (nếu có): .....

2.4. Kết quả rà quét, bóc gỡ mã độc:

Địa chỉ IP của đơn vị có nằm trong mạng máy tính ma (botnet) hay không? (nếu có, ghi rõ địa chỉ IP tĩnh của đơn vị):.....

Số lượng máy tính, thiết bị được rà quét: .....

---

[1] Trường hợp đã xây dựng, ghi rõ số hiệu văn bản

[2] Trường hợp đã ban hành, ghi rõ số văn bản

[3] Trường hợp đã ban hành, ghi rõ số văn bản

Số mã độc được phát hiện và xử lý:.....

- Khó khăn, vướng mắc (nếu có): .....

- Đề xuất, kiến nghị (nếu có): .....