CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

CẨM NANG AN TOÀN THÔNG TIN

DÀNH CHO KHỐI CÁC CƠ QUAN, ĐƠN VỊ

Mục lục

MÃ ĐỘC LÀ GÌ?

1

Mã độc (còn gọi là virus) là chương trình hoặc đoạn mã đưa vào máy tính, điện thoại, các thiết bị mạng hoặc bất kỳ thiết bị điện tử, phần mềm, ứng dụng trong hệ thống thông tin (có kết nối mạng hoặc không có kết nối mạng) nhằm thực hiện các hành vi trái phép (như ăn trộm dữ liệu, thông tin trên máy tính, điện thoại bị lây nhiễm, gửi thư rác, hay tham gia các cuộc tấn công mạng dưới điều khiển của Hacker hoặc tiếp tục phát tán mã độc khác).

MÃ ĐỘC LÀ GÌ?

Như vậy đối với người dùng Internet mã độc giống như kẻ xấu, khi đã lây nhiễm thành công vào máy tính, điện thoại di động, mã độc có thể làm bất cứ việc gì như:

- Theo dõi hoạt động của bạn trên các thiết bị này;
- Phá hủy dữ liệu (xóa dữ liệu, mã hóa dữ liệu ...);
- Đánh cắp dữ liệu, thông tin, tài khoản bạn đăng nhập, sử dụng lưu trữ trên máy tính, điện thoại di động, để đe dọa, tống tiền.
- Ghi âm cuộc gọi, đọc trộm tin nhắn ... thậm chí còn có thể theo dõi, chụp hình xung quanh nếu thiết bị có chức năng chụp hình.

NGUỒN LÂY NHIỄM MÃ ĐỘC

Bạn có thể bị mã độc tấn công bất cứ lúc nào nếu như:

- Không cảnh giác trong lúc sử dụng Intertnet để làm việc, học tập, giải trí, trò chuyện với bạn bè từ đó vô tình truy cập vào những đường dẫn độc hại, mở những tập tin có đính kèm mã độc, hay cài đặt phần mềm không tin cậy.
- Máy tính, điện thoại hoặc những phần mềm bạn đang sử dụng trên các thiết bị này có những điểm yếu, lỗ hổng mà mã độc có thể khai thác và xâm nhập vào máy tính của bạn
- Ngay cả khi bạn đã cảnh giác, đã biết cách bảo vệ máy tính, vẫn có những trường hợp bạn bị tấn công có chủ đích và bị cài cắm mã độc, tuy nhiên những trường hợp này rất ít xảy ra với người dùng bình thường.

NGUỒN LÂY NHIỄM MÃ ĐỘC

Dưới đây là một số nguồn lây nhiễm mã độc chính bạn cần biết để ngăn chặn mã độc lây nhiễm vào máy tính, điện thoại của mình:

- Các trang web lưu trữ tập tin độc hại/mã khai thác trên toàn thế giới, các trang web này có thể do Hacker chiếm quyền điều khiển hoặc cố tình dựng lên sau đó sử dụng để phát tán mã độc.
- Thư điện tử có đính kèm tập tin hoặc nội dung thư có đường dẫn độc hại
- Lỗ hổng phần mềm: Lỗ hổng, lỗi phần mềm cho phép Hacker truy cập từ xa vào máy tính người dùng, từ đó cài cắm mã độc, lấy trộm dữ liệu.
- Phương tiện lưu trữ di động, các ổ đĩa USB cũng là hình thức phổ biến để cài cắm mã độc vào máy tính người dùng.
- Phần mềm, ứng dụng miễn phí có đính kèm sẵn mã độc. Khi người dùng cài đặt phần mềm, ứng dụng này thì đồng thời cũng cài đặt mã độc vào máy tính, điện thoại của mình.

DẤU HIỆU THIẾT BỊ NHIỄM MÃ ĐỘC

Đối với những mã độc tinh vi

Người dùng thông thường (người không có kiến thức chuyên sâu về an toàn thông tin) rất khó có thể phát hiện ra, thậm chí những phần mềm phòng chống mã độc cũng không phát hiện. Tuy nhiên những trường hợp này rất ít xảy ra với người dùng bình thường.

Đối với những mã độc thông thường

Hầu hết các phần mềm phòng chống mã độc (còn gọi là anti-virus) sẽ cảnh báo cho người dùng và xử lý
Tuy nhiên nếu không dùng bất kỳ phần mềm phòng chống mã độc nào, hoặc có cài nhưng không sử dụng bạn có thể lưu ý những dấu hiệu sau:

- Máy tính, điện thoại chạy chậm, hoạt động không ổn định: mã độc lây nhiễm vào máy có thể gây ảnh hưởng đến hoạt động máy.
- Liên tục gặp lỗi khi mở tập tin trong ổ đĩa, đây có thể là một dấu hiệu đáng ngờ, cảnh báo nguy cơ mã độc đã bị cài cắm vào máy tính.
- Xuất hiện tập tin, ứng dụng, phần mềm lạ trên máy tính mặc dù không hề cài đặt.
- Dữ liệu trên máy tính, điện thoại đột nhiên bị mã hóa không mở được.
- Liên tục nhận được các cảnh báo giả
- Ổ cứng nhanh hết dung lượng trống
- Trình duyệt bị thay đổi bất thường, thanh công cụ mới xuất hiện dù không cài, những website tự động truy cập dù không gõ địa chỉ.
- Nhận được cảnh báo từ nhà cung cấp dịch vụ Internet hoặc các cơ quan chức năng.

HƯỚNG DẪN PHÒNG CHỐNG VÀ TIÊU DIỆT MÃ ĐỘC

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), thuộc Cục An toàn thông tin hướng dẫn người dùng internet các cơ quan, đơn vị và doanh nghiệp thực hiện 5 bước tham gia "Chiến dịch làm sạch mã độc trên không gian mạng":

BƯỚC 1: CHỌN THAM GIA CHIẾN DỊCH

Người dùng truy cập vào trang khonggianmang.vn/chiendichmadoc2022. Nhấn nút "Tham gia ngay".

BƯỚC 2: KIỂM TRA MỨC ĐỘ AN TOÀN MẠNG

Để kiểm tra mức độ an toàn mạng, người dùng bấm vào nút "Quét".

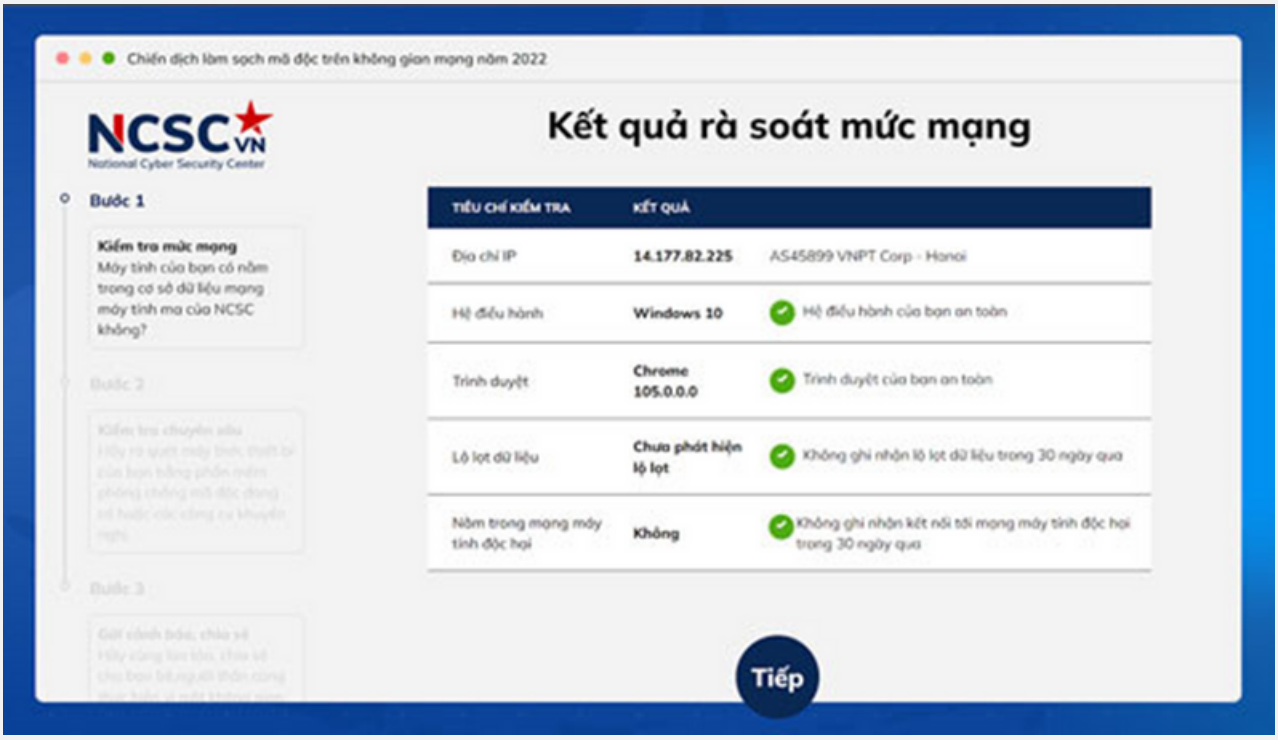
Khi đó, các chuyên gia NCSC sẽ giúp người dùng kiểm tra mã độc mức mạng trên thiết bị kết nối Internet và xác minh xem mạng đang dùng có nằm trong cơ sở dữ liệu mạng máy tính ma (botnet) hay không.

Đồng thời, rà soát điểm yếu, lỗ hổng của trình duyệt và hệ điều hành. Với bước này, người dùng có thể phát hiện máy tính, thiết bị kết nối Internet đang sử dụng có bị lộ lọt dữ liệu hay không.

Với bước này, người dùng có thể phát hiện máy tính, thiết bị kết nối Internet đang sử dụng có bị lộ lọt dữ liệu hay không.

Thời gian rà quét có thể trong vài giây đến vài phút, tùy thuộc vào tốc độ đường truyền Internet và cấu hình máy tính, thiết bị.

Hệ thống sẽ hiển thị thông tin kết quả rà quét với các tiêu chí gồm: thông tin về địa chỉ mạng (IP); mức độ an toàn của Hệ điều hành được cài đặt trên máy tính, thiết bị; mức độ an toàn của trình duyệt được sử dụng để vào Internet; mức độ lộ lọt dữ liệu trong 30 ngày kể từ thời điểm rà quét; mức độ an toàn của mạng máy tính được sử dụng.



Hệ thống hiển thị thông tin kết quả rà quét với nhiều tiêu chí.

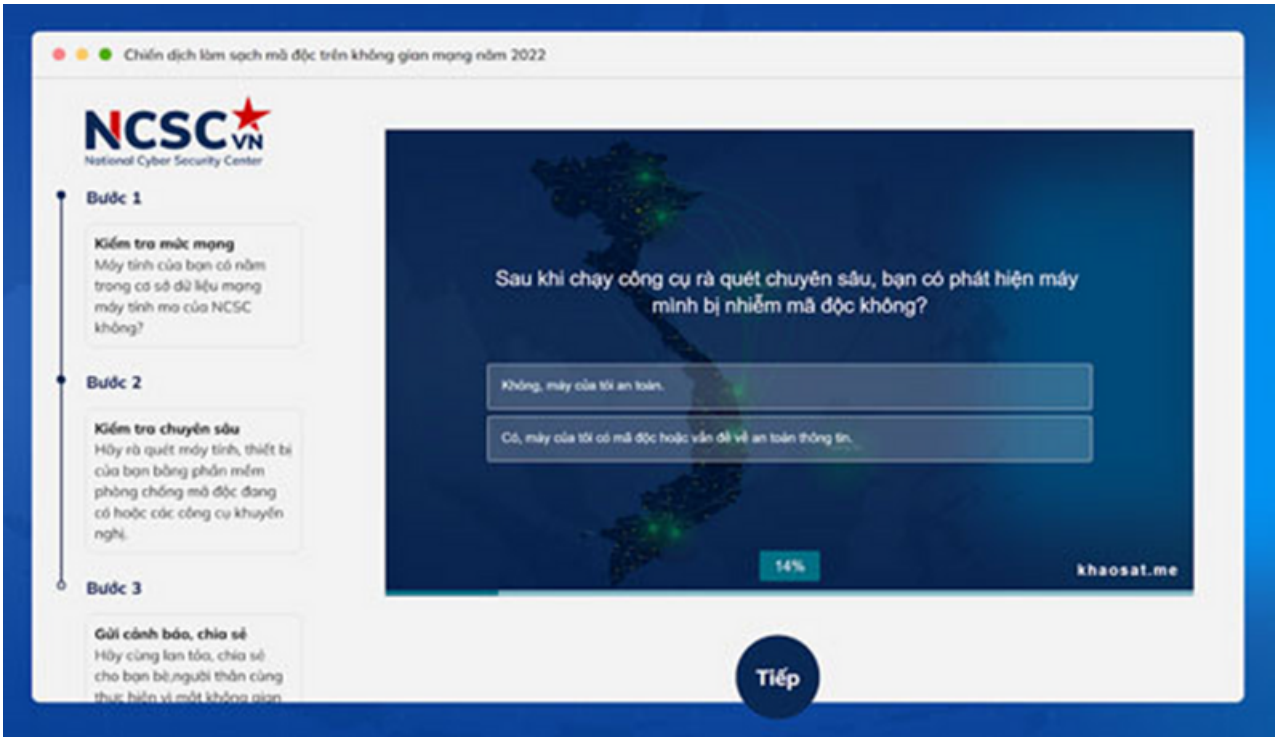
BƯỚC 3 - KIỂM TRA MÃ ĐỘC SỬ DỤNG CÔNG CỤ RÀ QUÉT CHUYÊN SÂU

Thời gian rà quét có thể trong vài giây đến vài phút, tùy thuộc vào tốc độ đường truyền Internet và cấu hình máy tính, thiết bị.

Hệ thống sẽ hiển thị thông tin kết quả rà quét với các tiêu chí gồm: thông tin về địa chỉ mạng (IP); mức độ an toàn của Hệ điều hành được cài đặt trên máy tính, thiết bị; mức độ an toàn của trình duyệt được sử dụng để vào Internet; mức độ lộ lọt dữ liệu trong 30 ngày kể từ thời điểm rà quét; mức độ an toàn của mạng máy tính được sử dụng.

BƯỚC 4 - XÁC NHẬN HOÀN THÀNH VÀ PHẢN ẢNH KẾT QUẢ

Đây là bước người dùng thông tin lại kết quả thực hiện việc rà quét. Kích chọn phương án trả lời hệ thống đưa ra dựa trên kết quả rà quét vừa làm.



Người dùng xác nhận hoàn thành việc tham gia và phản ánh kết quả tới hệ thống.

Kết thúc quá trình phản ảnh kết quả, người dùng bấm nút “Tiếp” để chuyển sang bước tiếp theo.

BƯỚC 5 - CHIA SẺ CHIẾN DỊCH

Bước cuối cùng này nhằm mục đích lan tỏa “Chiến dịch làm sạch mã độc trên không gian mạng” trong cộng đồng. Người dùng có thể chia sẻ, lan tỏa chiến dịch thông qua mạng xã hội đến người thân, bạn bè bằng việc kích chọn mục "Chia sẻ Facebook".

www.ais.gov.vn

CỤC AN TOÀN THÔNG TIN

Địa chỉ: Tầng 8 Toà nhà Cục Tần số vô tuyến điện, 115 Trần Duy Hưng, Phường Trung Hoà, Quận Cầu Giấy, TP.Hà Nội
Điện thoại: 024.39436684
Email: vanthucattt@mic.gov.vn