**Tài liệu**

**HƯỚNG DẪN GIÁM SÁT, NGĂN CHẶN KHẨN CẤP HỆ THỐNG MÁY CHỦ ĐIỀU KHIỂN MÃ ĐỘC TẤN CÔNG CÓ CHỦ ĐÍCH APT**

*(Kèm theo Công văn số /STTTT-BCVTCNTT ngày / /2024*

*của Sở Thông tin và Truyền thông)*

APT (Advanced Persistent Threat) là hình thức tấn công mạng có mục tiêu cụ thể do tin tặc chọn, sử dụng các công nghệ tiên tiến và kỹ thuật lừa đảo để đột nhập mạng mục tiêu và dai dẳng tập trung vào mục tiêu đó trong nhiều tuần, nhiều tháng hoặc nhiều năm cho đến khi cuộc tấn công diễn ra thành công (hoặc bị chặn đứng). Một khi vào được trong mạng, tin tặc cố giấu mình để không bị phát hiện trong khi sử dụng một số loại phần mềm độc hại (malware) để đánh cắp thông tin quan trọng phục vụ cho các mục đích xấu.

**I. Dấu hiệu nhận biết máy tính nhiễm malware**

1. Các trang quảng cáo popup xuất hiện, ngay cả khi không bật trình duyệt.
2. Điều hướng trình duyệt bị thay đổi.
3. Chương trình bảo mật bạn chưa bao giờ cài đặt trên máy xuất hiện những cảnh báo đáng sợ.
4. Có những bài viết lạ trên mạng xã hội của bạn mà không phải là do bạn viết hay chia sẻ.
5. Xuất hiện một chương trình kiểm soát máy tính của bạn và đòi tiền chuộc.
6. Đột nhiên bạn không thể sử dụng các công cụ hệ thống phổ biến (cmd, taskmanager…).

**II. Gỡ bõ malware khỏi máy tính bị lây nhiễm**

Khi máy tính có biểu hiện lây nhiễm malware, thực hiện việc gỡ bỏ theo 2 bước sau:

1. Cập nhật phiên bản mới nhất của chương trình diệt virus trên máy, chạy tính năng “full scan” , sau khi kiểm tra kết quả, nếu máy tính vẫn xuất hiện những dấu hiệu của việc lây nhiễm, thực hiện sang bước thứ 2 dưới đây.

2. Gỡ bỏ malware theo quy trình 4 bước :

- Vào Safe Mode: Ngắt kết nối intenet, khởi động lại máy và vào tính năng Safe Mode (Tùy theo phiên bản windows sẽ có những cách vào Safe Mode khác nhau).

- Xóa các file tạm (temporary files): sử dụng chương trình Disk Cleanup đi kèm với windows. Việc xóa các file tạm sẽ làm tăng tốc độ quét virus, giải phóng ổ đĩa, thậm chí có thể loại vỏ một vài malware.

- Cài đặt chương trình quét malware: tải về chương trình theo địa chỉ: <https://www.malwarebytes.com/mwb-download/>.

- Thực hiện quét virus với chương trình Malwarebytes vừa cài đặt.

**III. Thực hiện ngăn ngừa lây nhiễm mã độc từ các địa chỉ IP và Domain theo danh sách khuyến cáo của Cục ATTT**

1. **Đối với máy tính cá nhân:**

- Cập nhật các lỗ hổng: Theo khuyến cáo của Cục ATTT

- Thực hiện thay đổi file host trong thư mục C:\Windows\System32\drivers\etc (cần sử dụng quyền Administrator) để khóa kết nối tới các trang web và các IP Server lây nhiễm theo danh sách đính kèm từ công văn của Cục ATTT theo minh họa dưới đây:

- Sử dụng notpad mở file host trong thư mục C:\Windows\System32\drivers\etc

- Tham khảo bài viết tại ***https://www.thegioididong.com/hoi-dap/chan-website-bat-ky-tren-may-tinh-1163897*** (mục đích để ngăn kết nối tới các trang web lây nhiễm đã được khuyến cáo).

- Ghi chú: Thực hiện Save file host sau khi đã chỉnh sửa như trên, lặp lại việc thêm vào toàn bộ các địa chỉ được khuyến cáo theo danh sách đính kèm của Cục ATTT để khóa toàn bộ kết nối với các trang web lây nhiễm.

**2.** **Với hệ thống mạng:**

**-** Thực hiện việc khóa kết nối với các trang web và máy chủ lây nhiễm thông qua chức năng “Filter” trên modem của nhà cung cấp dịch vụ Internet:

- Đăng nhập vào giao diện quản trị modem.

- Tìm đến chức năng Filter và thực hiện việc thêm vào các trang web hay các IP được khuyến cáo lây nhiễm.

-Thực hiện tương tự với các IP lây nhiễm được khuyến cáo.

- Ghi chú: Tùy theo loại modem mà tính năng “Filter” có thể có khác biệt nhất định. ***Tham khảo bài viết tại https://quantrimang.com/cong-nghe/huong-dan-chan-website-voi-router-tp-link-116818***