



HIỂU VỀ VIRUS MÁY TÍNH

COMPUTER VIRUS

FUNIX A member of
Learn with the expert

By:

NGUYỄN THÀNH DOANH

MỤC LỤC

1. Tác Hại Của Virus Máy Tính	4
2. Phân Loại Virus Máy Tính	4
2.1. Web Scripting Virus	4
2.1.1. Đặc điểm của virus	4
2.1.2. Khía cạnh hoạt động của máy tính bị virus khai thác	4
2.1.3. Cách thức lây lan	4
2.1.4. Cách thức phòng chống	4
2.2. Virus File	4
2.2.1. Đặc điểm của virus	4
2.2.2. Khía cạnh hoạt động của máy tính bị virus khai thác	5
2.2.3. Cách thức lây lan	5
2.2.4. Cách thức phòng chống	5
2.3. Virus Macro	5
2.3.1. Đặc điểm của virus	5
2.3.2. Khía cạnh hoạt động của máy tính bị virus khai thác	5
2.3.3. Cách thức lây lan	5
2.3.4. Cách thức phòng chống	6
2.4. Trojan Horse	6
2.4.1. Đặc điểm của virus	6
2.4.2. Khía cạnh hoạt động của máy tính bị virus khai thác	6
2.4.3. Cách thức lây lan	6
2.4.4. Cách thức phòng chống	6

2.5. Computer Worm.....	6
2.5.1. <i>Đặc điểm của virus</i>	6
2.5.2. <i>Khía cạnh hoạt động của máy tính bị virus khai thác</i>	7
2.5.3. <i>Cách thức lây lan</i>	7
2.5.4. <i>Cách thức phòng chống</i>	7
3. Bảng So Sánh Virus File, Trojan Horse Và Computer Worm	7
4. Minh Họa Hoạt Động Đảm Bảo Máy An Toàn	8
4.1. Lập Luận Chứng Minh Máy Tính Sạch	8
4.1.1. <i>Sử dụng phần mềm diệt virus</i>	8
4.2. Kinh Nghiệm Giữ Cho Máy Tính Không Bị Nhiễm Virus	9
Tài Liệu Tham Khảo	10

1. TÁC HẠI CỦA VIRUS MÁY TÍNH

- Tiêu tốn tài nguyên hệ thống
- Phá hủy hệ thống
- Mã hóa dữ liệu để tống tiền
- Đánh cắp dữ liệu
- Phá hủy dữ liệu
- Gây khó chịu cho người dùng

2. PHÂN LOẠI VIRUS MÁY TÍNH

2.1. WEB SCRIPTING VIRUS

2.1.1. ĐẶC ĐIỂM CỦA VIRUS

- Gồm hai loại:
 - Persistent: Có khả năng mạo danh người dùng và gây nhiều thiệt hại
 - Non-Persistent: Có khả năng tấn công mà chúng ta không hề biết
- Có thể lây lan với tốc độ cực nhanh

2.1.2. KHÍA CẠNH HOẠT ĐỘNG CỦA MÁY TÍNH BỊ VIRUS KHAI THÁC

- Khai thác các lỗ hổng trình duyệt và vi phạm các bảo mật trình duyệt

2.1.3. CÁCH THỨC LÂY LAN

- Thông qua các quảng cáo bị nhiễm mã độc
- Được gửi dưới dạng tệp đính kèm trong email
- Thông qua các thông báo pop-up
- Thông qua các chương trình chạy trên web

2.1.4. CÁCH THỨC PHÒNG CHỐNG

- Không mở các email từ các nguồn đáng ngờ và không xác định
- Tránh truy cập trang web của bên thứ ba
- Chỉ sử dụng các trang web chính thức để tải phần mềm

- Không nhấp vào quảng cáo liên tục trong cửa sổ trình duyệt
- Sử dụng chương trình Chrome Anti Malware

2.2. VIRUS FILE

2.2.1. ĐẶC ĐIỂM CỦA VIRUS

- Chỉ tiến hành lây lan trên những file thi hành được
- Lây lan nhanh và khó diệt hơn các loại virus khác

2.2.2. KHÍA CẠNH HOẠT ĐỘNG CỦA MÁY TÍNH BỊ VIRUS KHAI THÁC

- Chạy các chương trình

2.2.3. CÁCH THỨC LÂY LAN

- Lây nhiễm vào các chương trình
- Khi mở file bị nhiễm virus, virus sẽ tự động kích hoạt và lây nhiễm sang các file khác

2.2.4. CÁCH THỨC PHÒNG CHỐNG

- Không cài đặt hoặc mở những file không rõ nguồn gốc
- Cập nhật Window thường xuyên
- Kiểm tra và quét virus định kỳ

2.3. VIRUS MACRO

2.3.1. ĐẶC ĐIỂM CỦA VIRUS

- Đặc biệt tấn công vào chương trình trong bộ Microsoft Office
- Có thể tự sao chép và lây nhiễm sang các máy tính khác

2.3.2. KHÍA CẠNH HOẠT ĐỘNG CỦA MÁY TÍNH BỊ VIRUS KHAI THÁC

- Chạy các chương trình trong bộ Microsoft Office

2.3.3. CÁCH THỨC LÂY LAN

- Lây nhiễm vào các file văn bản, bảng tính...trong bộ Microsoft Office
- Lây lan qua các thư rác (spam email)

2.3.4. CÁCH THỨC PHÒNG CHỐNG

- Không mở các file đính kèm từ các nguồn không đáng tin cậy
- Sử dụng bộ chương trình Microsoft Office mới nhất
- Kiểm tra và quét virus định kì

2.4. TROJAN HORSE

2.4.1. ĐẶC ĐIỂM CỦA VIRUS

- Trojan là một đoạn mã chương trình hoàn toàn không có tính chất lây lan
- Được ngụy trang bằng một vỏ bọc tưởng chừng vô hại để tạo tin tưởng cho người dùng

2.4.2. KHÍA CẠNH HOẠT ĐỘNG CỦA MÁY TÍNH BỊ VIRUS KHAI THÁC

- Chạy chương trình

2.4.3. CÁCH THỨC LÂY LAN

- Lây nhiễm từ đường dẫn hoặc file đính kèm trong mail
- Lợi dụng các lỗ hổng trong trình duyệt web, phần mềm hoặc ứng dụng nhắn tin
- Chúng đi theo các phần mềm, games miễn phí không đáng tin cậy hay các phần mềm bẻ khóa (crack, keygen)

2.4.4. CÁCH THỨC PHÒNG CHỐNG

- Không mở các file đính kèm từ các nguồn không đáng tin cậy
- Không tải về các phần mềm khi chưa biết rõ nguồn gốc do ai viết, có virus hay không, phần mềm có yêu cầu truy cập quyền riêng tư người dùng không.
- Không bấm trực tiếp vào các đường link rút gọn đuôi adf.ly hoặc các link rút gọn khác được chia sẻ trên forum, mạng xã hội.
- Cập nhật bản vá lỗ hổng thường xuyên cho Windows và các phần mềm khác
- Bật tường lửa và sử dụng trình diệt virus

2.5. COMPUTER WORM

2.5.1. ĐẶC ĐIỂM CỦA VIRUS

- Là loại virus có sức lây lan rộng, nhanh và phổ biến nhất hiện nay
- Worm kết hợp cả sức phá hoại của virus, đặc tính âm thầm của Trojan
- Có khả năng tự nhân bản

2.5.2. KHÍA CẠNH HOẠT ĐỘNG CỦA MÁY TÍNH BỊ VIRUS KHAI THÁC

- Chạy chương trình
- Các lỗ hổng ẩn trong hệ điều hành (OS) máy tính của bạn

2.5.3. CÁCH THỨC LÂY LAN

- Thâm nhập thông qua đĩa mềm hoặc các thiết bị lưu trữ khác(usb, ổ cứng rời,...)
- Thâm nhập qua các tệp đính kèm trong email, mạng xã hội, dịch vụ nhắn tin tức thời, hoặc qua các phương thức chia sẻ tệp.

2.5.4. CÁCH THỨC PHÒNG CHỐNG

- Không mở các file đính kèm từ các nguồn không đáng tin cậy
- Không nhấp vào các liên kết lạ
- Không nhấp vào các quảng cáo sơ sài
- Cập nhật hệ điều hành mới nhất
- Kiểm tra và quét virus định kì

3. BẢNG SO SÁNH VIRUS FILE, TROJAN HORSE VÀ COMPUTER WORM

		Virus File	Trojan Horse	Computer Worm
GIỐNG	<i>Cách Lây Nhiễm</i>	<ul style="list-style-type: none">• Lây nhiễm thông qua tệp đính kèm trong mail, chạy các chương trình nhiễm mã độc		
	<i>Mục Tiêu Phá Hoại</i>	<ul style="list-style-type: none">• Phá hủy, ăn cắp dữ liệu của người dùng• Gây khó chịu cho người sử dụng		

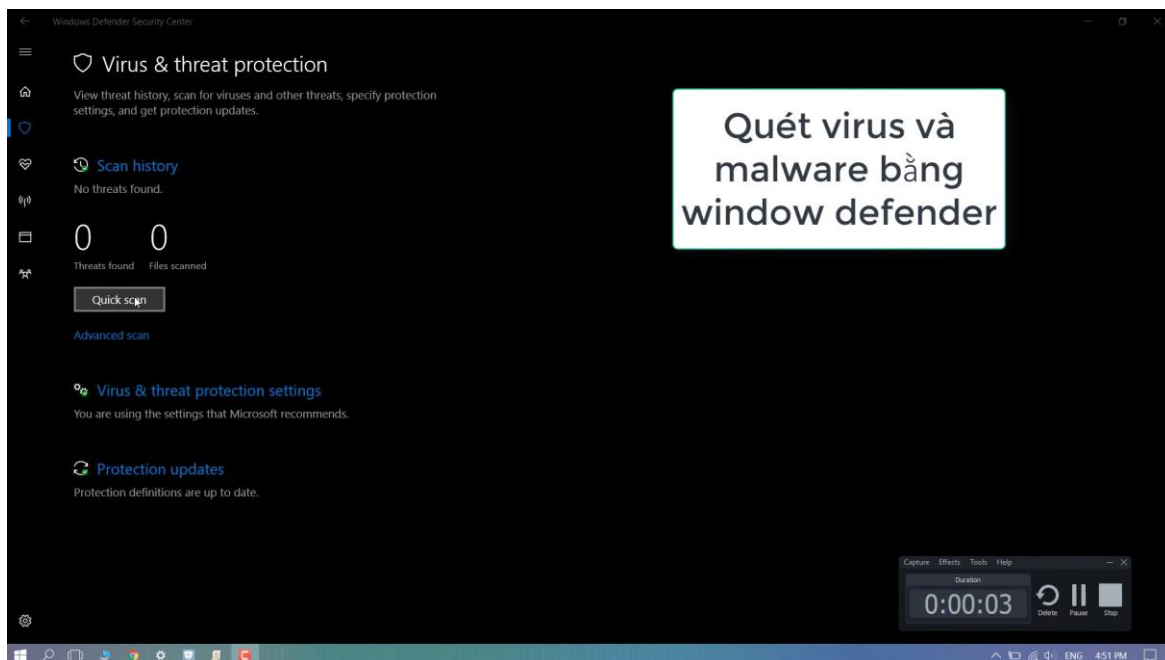
KHÁC	<i>Cách lây Nhiễm</i>	Chạy chương trình đã bị nhiễm virus cũng là lúc virus được kích hoạt và tiếp tục tìm các file chương trình khác trong máy của bạn để lây vào	Không tự lây lan. Nhưng có thể lây nhiễm bằng cách đi kèm với các virus khác, đặc biệt dạng Worm để xâm nhập	Có thể lây lan qua các dịch vụ gửi tin nhắn tức thời, hoặc thông qua lỗ hổng phần mềm
	<i>Mục Tiêu Phá Hoại</i>	Mã hóa dữ liệu trong máy tính	Phá hủy hoặc đánh cắp dữ liệu	Mã hóa dữ liệu và tổng tiền nạn nhân

4. MINH HỌA HOẠT ĐỘNG ĐẢM BẢO MÁY AN TOÀN

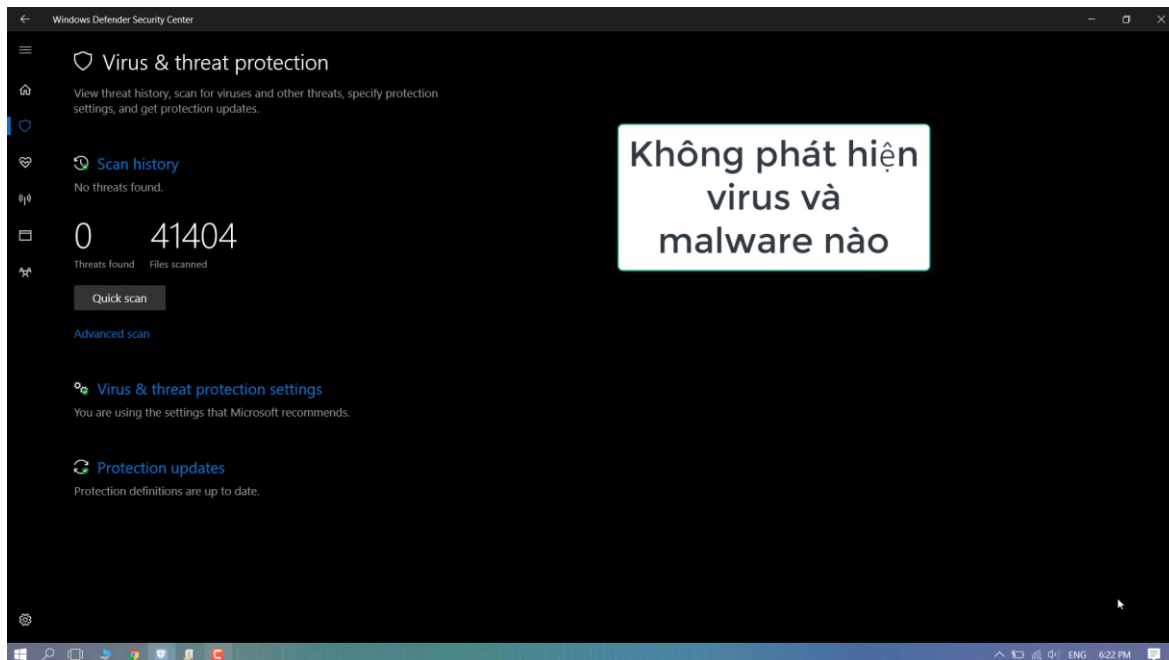
4.1. LẬP LUẬN CHỨNG MINH MÁY TÍNH SẠCH

4.1.1. SỬ DỤNG PHẦN MỀM DIỆT VIRUS

- Sử dụng Window Defender



- Tiến hành quét toàn bộ máy tính và thông báo sau khi quét xong (Quick Scan)



- Không tìm thấy bất kì mối nguy hiểm hay Virus gây hại nào.

⇒ **Máy tính sạch sẽ, không có virus !**

4.2. KINH NGHIỆM GIỮ CHO MÁY TÍNH KHÔNG BỊ NHIỄM VIRUS

- Không click vào các tệp tin, đường dẫn trong email được gửi từ người lạ.
- Sử dụng phần mềm diệt virus và giữ cho phần mềm luôn cập nhật.
- Cập nhật bản vá lỗi hỏng thường xuyên cho Windows và các phần mềm khác.
- Không cài đặt hoặc mở những file không rõ nguồn gốc.
- Không sử dụng các phần mềm lậu và công cụ bẻ khóa.

TÀI LIỆU THAM KHẢO

- Computer virus – Wikipedia.org
- Web scripting virus - internetsecurity.tips - geeksforgeeks.org
- Các loại virus máy tính – Bkav.com.vn
- Mã độc là gì? 12 loại mã độc phổ biến - securitybox.vn
- Trojan Horse - securitybox.vn
- What is a computer worm? – avast.com