Lớp : CR 210T

Nhóm : 9

Thành viên nhóm 9

Trần Thế Tường - 27211239157

Phạm Quang Ngà – 0966

**Bài báo cáo**

* **Mục lục**
* Biện pháp phòng tránh virus máy tính
* Cấu tạo và chức năng nguyên lý hoạt động của virus
* **Cách WannaCry lây nhiễm trên diện rộng**
* Ưu điểm & nhược điểm
* Các lỗi
* Cách khắc phục

**Chủ đề :** Virus máy tính, và cách phòng chống

- Thời buổi hiện nay công nghệ 4.0 phát triển nhiều thiết bị, máy tính hiện đại ra đời bên cạnh đó cũng có một số điểm tiêu cực làm hại tới những thiết bị và máy tính và một trong những yếu tố ảnh hưởng nhiều nhất đến an toàn của thông tin máy tính, thiết bị là virus máy tính.

- Khái niệm về virus : Virus máy tính là một chương trình hay một đoạn chương trình có khả năng tự nhân bản hay sao chép chính nó từ đối tượng bị lây nhiễm này sang đối tượng khác mỗi khi đối tượng bị lây nhiễm bị kích hoạt.

- Một số virus máy tính phổ biến bao gồm : Wanna cry virus, Code Red, Crypto Locker, Creeper virus ...

* **Biện pháp phòng tránh virus máy tính**

- Cài đặt phần mềm diệt virus, sử dụng bảng hệ thống, tắt tự động cài đặt, tạo lớp bảo vệ, không nhập vào các nút tải xuống không cần thiết và không chạy các chương trình từ Internet hoặc sao chép từ máy tính khác, sử dụng trình duyệt web an toàn, nhắc nhở các cảnh báo virus xuất hiện, cài đặt các bản cập nhật mới nhất từ Microsoft Update và luôn luôn làm mới phần mềm.

- Định kỳ quét và diệt virus bằng các phần mềm diệt virus.

* **Cấu tạo và chức năng nguyên lý hoạt động của virus**

**-** Hiện nay có rất nhiều virus máy tính xuất hiện trên máy tính và các nền tảng với nhiều cơ chế và chức năng, nguyên lý hoạt động khác nhau sau đây là một con virus điển hình từng khuấy đảo trên máy tính. Đó là virus Wannacry.

**- WannaCry là gì?**

**-** WannaCry là một loại mã độc tống tiền (ransomware), với các tên gọi khác nhau như WannaCrypt0r 2.0 hay WCry. Phần mềm độc hại này mã hóa dữ liệu của máy tính và ngăn cản người dùng truy cập dữ liệu trên đó cho đến khi tin tặc nhận được tiền chuộc. Các chuyên gia cho rằng, mã độc này nguy hiểm vì, nó hỗ trợ tin tặc “giữ” dữ liệu của người dùng làm “con tin” để tống tiền các cá nhân hoặc tổ chức/doanh nghiệp. Việc làm này được cho là hiệu quả hơn việc đánh cắp hoặc xóa đi dữ liệu trên máy tính.

**- Cơ chế hoạt động của Virus WannaCry**

**-** Khi được cài đặt vào máy tính, WannaCry sẽ tìm kiếm các tập tin (thông thường là các tập tin văn bản) trong ổ cứng và mã hóa chúng, sau đó để lại cho chủ sở hữu một thông báo yêu cầu trả tiền chuộc nếu muốn giải mã dữ liệu. Mã độc WannaCry khai thác lỗ hổng của hệ điều hành Windows mà Cơ quan An ninh Quốc gia Mỹ (NSA) đã nắm giữ. Tội phạm mạng đã sử dụng chính những công cụ của NSA để phát tán và lây lan mã độc.

* **Cách WannaCry lây nhiễm trên diện rộng**

**-** WannaCry có 2 cách thức lây lan chính :

- Cách 1: Phát tán qua phương thức thông thường là đính kèm vào các bản “bẻ khóa” của phần mềm rồi chia sẻ lên các trang web có nhiều người truy cập. Mục đích là để người dùng tải về và kích hoạt hoặc truy cập vào các trang web độc hại để lây nhiễm mã độc. Về mặt kỹ thuật, WannaCry phát tán qua các mạng lưới phát tán mã độc và bộ khai thác Exploit Kit.

- Cách 2: Lây lan qua mạng LAN bằng cách khai thác các lỗ hổng EternalBlue của dịch vụ SMB mà NSA phát triển bí mật, nhưng sau đó đã bị nhóm tin tặc ShadowBroker đánh cắp và phát hành công khai. Cách này đã làm cho WannaCry lây lan một cách nhanh chóng trên toàn thế giới.

* **Ưu điểm & nhược điểm**

- Về ưu điểm thì virus WannaCry không có ưu điểm. Thực tế, nó là một mối đe dọa lớn đối với các tổ chức và cá nhân trên toàn thế giới và đã gây ra nhiều tổn hại và thiệt hại .

- Nhược điểm của virus WannaCry bao gồm :

- WannaCry là một loại ransomware, có chức năng mã hóa các tập tin trên máy tính của nạn nhân và yêu cầu đền tiền chuộc để giải mã. Điều này gây ra tổn thất nặng nề cho các doanh nghiệp và cá nhân bị tấn công.

- Virus này đã lây lan nhanh chóng trên toàn cầu và tấn công nhiều doanh nghiệp, tổ chức, cơ quan chính phủ ở hơn 150 quốc gia.

- Nó đã khai thác một lỗ hổng bảo mật trong Windows mà Microsoft đã phát hành một bản vá chỉ vài tháng trước đó.

- Một số chiến lược chống lại WannaCry là không hiệu quả, bao gồm cả việc đóng băng tài khoản Bitcoin và thanh toán tiền chuộc.

* **Các lỗi**

**-** Khi máy tính bị nhiễm virus wannacry thì sẽ bị mã hóa toàn bộ dữ liệu

- Giảm tốc độ máy tính : virus WannaCry sử dụng các tài nguyên của hệ thống và làm giảm tốc độ máy tính.

- Thiếu hụt dữ liệu : virus WannaCry có thể phá hủy dữ liệu trên các hệ thống mạng và gây thiếu hụt dữ liệu nghiêm trọng.

* **Cách khắc phục**

**-** Cập nhật hệ thống của bạn: WannaCry khai thác các lỗ hổng trong hệ điều hành Windows cũ đối với phần mềm như Windows XP, Windows 8, Windows Server 2003, và Windows Server 2008, vì thế bạn cần cập nhật hệ điều hành của mình lên phiên bản mới nhất để khắc phục lỗ hổng bảo mật đó.  
- Cài đặt và cập nhật phần mềm diệt virus: Bạn nên cài đặt phần mềm diệt virus để phát hiện và loại bỏ WannaCry cũng như các loại mã độc khác trên hệ thống của bạn. Ngoài ra, bạn cũng cần thường xuyên cập nhật phần mềm diệt virus để đảm bảo tính hiệu quả của nó.  
- Thực hiện sao lưu dữ liệu: Nếu bị tấn công bởi WannaCry, dữ liệu trên máy tính của bạn có thể bị mất mát hoặc bị mã hóa, vì vậy bạn cần sao lưu dữ liệu thường xuyên để đảm bảo việc phục hồi dữ liệu khi cần thiết.  
- Tắt tính năng SMBv1: WannaCry sử dụng giao thức SMBv1 để lây lan qua mạng, bạn có thể tắt tính năng này trên máy tính của bạn.