

CHƯƠNG 3.

An toàn phần mềm

Phần mềm ác tính

Lỗi phần mềm

3.1. Phần mềm ác tính – Malware

- Phần mềm ác tính là gì?
- Phần mềm ác tính thường gặp
- Virut.
- Biện pháp ngăn chặn
- Một số ngộ nhận

3.1.1. Phần mềm ác tính là gì

- ❑ Chạy theo chủ định người lập trình
- ❑ Chạy và phản ứng theo cách bất thường, không trông đợi từ phía người dùng.
- ❑ Ân náu trong hệ thống, gắn vào các phần mềm không ác tính
- ❑ Có thể làm mọi thứ mà một phần mềm thông thường có thể

3.1.2. Phần mềm ác tính thường gặp

- Virus: Gắn vào một chương trình, phát tán bản sao ra các chương trình khác.
- Trojan horse: Có các tính năng bất thường
- Logic bom: Phát động khi điều kiện được thỏa
- Time bom: Phát động khi đến hạn thời gian.
- Backdoor: Cho phép truy nhập trái phép các tính năng
- Worm: Phát tán bản sao qua hình thức mạng
- Rabbit: Nhân bản đến khi cạn tài nguyên
- ...

3.1.3. Virus

❑ Kích hoạt Virus:

Virus chỉ gây hại khi được kích hoạt.

- Virus chạy cùng với một chương trình khác chạy bởi người dùng.
- Virus chạy khi mở tệp đính kèm trong e-mail, tệp ảnh, tệp đồ họa...

❑ Phát tán Virus:

Virus chỉ gây hại khi được kích hoạt.

- Virus chạy cùng với một chương trình khác chạy bởi người dùng.

3.1.3. Virus

- Phát tán Virus:
 - Mã Virus đính vào mã chương trình.
 - ✓ Nối mã Virus với mã chương trình.
 - ✓ Mã Virus bao quanh mã chương trình.
 - ✓ Mã Virus tích hợp vào mã chương trình.
 - Virus tài liệu
 - ✓ Tài liệu chứa cả dữ liệu và các lệnh.

3.1.3. Virus

- Nơi ẩn náu Virus:
 - Vùng Boot (Boot Sector)
 - Bộ nhớ (Memory-Resident)
 - Ứng dụng (Application Program)
 - Thư viện (Library)
 - ...

3.1.3. Virus

- Một số dấu hiệu nhận biết Virus:
 - Mã Virus có kiểu mẫu đặc biệt.
Có thể nhận biết các đoạn mã của từng loại Virus.
 - Mã đính kèm không thay đổi
Chương trình đính kèm sẽ lớn hơn chương trình ban đầu.
 - Vị trí đính kèm không thay đổi.

3.1.4. Các biện pháp ngăn chặn

- Sử dụng phần mềm thương mại từ nguồn tin cậy
- Kiểm thử phần mềm trên máy tính/hệ thống tách biệt.
- Mở tệp đính kèm chỉ khi biết rõ nguồn gốc
- Lưu ở nơi an toàn một phiên bản có thể tái tạo của hệ thống đang sử dụng.
- Sử dụng phần mềm quét, diệt phần mềm ác tính.

3.1.5. Một số ngộ nhận về phần mềm ác tính.

- ❑ Chỉ lây nhiễm trên các hệ thống Windows.
- ❑ Không thể thay đổi các tệp *hidden* hoặc *read-only*.
- ❑ Có thể lây nhiễm trên phần cứng.
- ❑ Chỉ phát tán thông qua disk, email.
- ❑ Không thể tồn tại trong bộ nhớ sau khi *reboot power off/on*.
- ❑ Chỉ xuất hiện trong các tệp dữ liệu, chương trình.

3.2. Lỗi phần mềm.

- ❑ Lỗi phần mềm là gì?
- ❑ Lỗi phần mềm thường gặp
- ❑ Các biện pháp an toàn

3.2.1. Lỗi phần mềm là gì.

- ❑ Lỗi do lập trình viên trong quá trình phát triển phần mềm:
 - Không có ý
 - Không ác tính
 - Đôi khi gây hậu quả nghiêm trọng

3.2.2. Lỗi phần mềm thường gặp.

- ❑ Tràn bộ đệm (Buffer Overflow)
- ❑ Không đầy đủ (Incomplete Mediation)
- ❑ Đồng bộ (Synchronization)

3.2.3. Các biện pháp an toàn.

- ❑ Kiểm thử (Testing)
- ❑ Kiểm định hình thức (Formal Verification)
- ❑ Lập trình an toàn (Secure Coding)

Cảm ơn!

